EPICenter Concepts and Solutions Guide

Version 5.0

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
http://www.extremenetworks.com

Published: October, 2004
Part number: 100175-00 Rev. 01

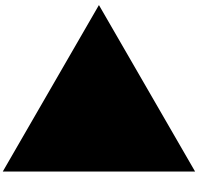
©2004 Extreme Networks, Inc. All rights reserved. Extreme Networks and BlackDiamond are registered trademarks of Extreme Networks, Inc. in the United States and certain other jurisdictions. EPICenter, ExtremeWare, ExtremeWare Vista, ExtremeWorks, ExtremeAssist, ExtremeAssist1, ExtremeAssist2, PartnerAssist, Extreme Standby Router Protocol, ESRP, SmartTraps, Alpine, Summit, Summit1, Summit4, Summit4/FX, Summit7i, Summit24, Summit48, Summit Virtual Chassis, SummitLink, SummitGbX, SummitRPS and the Extreme Networks logo are trademarks of Extreme Networks, Inc., which may be registered or pending registration in certain jurisdictions. The Extreme Turbodrive logo is a service mark of Extreme Networks, which may be registered or pending registration in certain jurisdictions. Specifications are subject to change without notice.

Solaris is a trademark of Sun Microsystems, Inc.

This product includes software developed by the Apache Software Foundation (http://www.apache.org).

This product contains copyright material licensed from AdventNet, Inc. (http://www.adventnet.com). All rights to such copyright material rest with AdventNet.

All other registered trademarks, trademarks and service marks are property of their respective owners.



Contents

Preface

Introduction **9**
Terminology 9

Conventions **10**

Related Publications **11**

Chapter 1 EPICenter Overview

Introduction **13**

EPICenter Features **13**
Inventory Management 15
The Alarm System 15
The Configuration Manager and the Firmware Manager 16
The Grouping Manager 16
The IP/MAC Address Finder 16
The Telnet Feature 16
Real-Time Statistics 17
Topology Views 17
Enterprise-wide VLAN Management 18
The ESRP Manager 18
The STP Monitor 18
EPICenter Reports 18
Role-based Access Management 19
EPICenter Stand-alone Utilities 19
The EPICenter Policy Manager Upgrade 19
Distributed Server Mode (EPICenter Gold Upgrade) 20

EPICenter Software Architecture **20**

Extreme Networks Switch Management **21**
SNMP and MIBs 21
Traps and Smart Traps 22
Device Status Polling 22

Extreme Networks Device Support 23
Third-Party Device Support 23

Chapter 2 Getting Started with EPICenter

Starting EPICenter **25**
Starting the EPICenter Server **25**
Starting the EPICenter Client 26
The EPICenter Client Login Window 28

Getting Help **30**

Working with the EPICenter Features **31**
Device Selection Persistence 31
Running Features in Separate Windows 32

EPICenter User Roles **32**

Creating the Device Inventory **33**
Using Discovery 33
Adding Devices Individually 35
Setting up Default Device Contact Information 35
Creating and Using Device Groups 35

Managing Device Configurations and Firmware **37**
Saving Baseline Configuration Files in the Configuration Manager 37
Scheduling Configuration File Archiving 39
Checking for Software Updates 40

Using the EPICenter Alarm System **41**
Predefined Alarms 41
The Alarm Log Browser 42
Filtering the Alarm Log Display 43
Creating or Modifying an Alarm Definition 46
Threshold Configuration for RMON and CPU Utilization Alarms 53
Configuring a CPU Utilization Rule 56

Using Topology Views **58**
Automated Map Creation vs. Manual Map Creation 60
Customizing the Look of Your Maps 61

Using Basic EPICenter Reports **61**

Chapter 3 Managing your Network Assets

Creating a Network Component Inventory **65**
Using Discovery to Find Network Devices 65
Adding Devices Individually 68
Importing Devices Using the DevCLI Utility 69

Making Device Contact Information Changes **69**

Organizing Your Inventory with Device Groups **71**

Monitoring Critical Links with Port Groups **72**

Inventory Reports **74**
Uploading Inventory Information to Extreme Networks 75

Chapter 4 Configuring and Monitoring Your Network

Scalable, Concurrent Multidevice Configuration **77**

User-Defined Telnet Macros **78**
Creating Telnet Macros for Re-Use 79
Creating Macros to be Run From a Menu 80
Role-based Telnet Macro Execution 81

Network-wide VLAN Configuration **82**

Graphical and HTML-based Configuration Monitoring **83**

Chapter 5 Managing VLANs

Graphical Configuration and Monitoring of VLANs **85**

Network-wide VLAN Membership Visibility **86**

Network-wide Multidevice VLAN Configuration **88**
Modifying VLANs from a Topology Map 89

Displaying VLAN Misconfigurations with Topology Maps **90**

Chapter 6 Managing Network Device Configurations and Updates

Archiving Component Configurations **93**

Baseline Configurations **94**
Identifying Changes in Configuration Files 95
Automatic Differences Detection 95

Device Configuration Management Log **96**

Managing Firmware Upgrades **97**
Automated Retrieval of Firmware Updates from Extreme Networks 97
Detection of Firmware Obsolescence for Network Components 97
Multi-Step Upgrade Management 97

Chapter 7 Managing Network Security

Security Overview **99**

Management Access Security **99**
Using RADIUS for User Authentication 100
Setting up EPICenter Roles using RADIUS 100
Securing Management Traffic 100

Monitoring Configuration Changes **102**

MAC Address Finder **103**

Using Alarms to Monitor Potential Security Issues **103**

Device Syslog History **104**

Network Access Security **105**
Using VLANs 105
Using IP Access Lists 107

Chapter 8 Managing Wireless Networks

Wireless Networking Overview **109**

Inventory Management Using Wireless Reports **110**

Security Monitoring with Reports **110**
Client MAC spoofing report 111
Monitoring Unauthenticated Clients 111

Detecting Rogue Access Points **112**
Enabling Rogue Access Point Detection 112

Detecting Clients with Weak or No Encryption **113**

Wireless Network Status with Reports **114**

Performance Visibility with Reports **114**

Debugging Access Issues with Syslog Reports **115**

Fault Isolation with Reports **115**

Chapter 9 Tuning and Debugging EPICenter

Monitoring and Tuning EPICenter Performance **117**
Polling Types and Frequencies 118
Performance of the EPICenter Server 119

Tuning the Alarm System **120**
Disabling Unnecessary Alarms 120
Limiting the Scope of Alarms 121
The Alarm and Event Log Archives 123

Using the MIB Poller Tools **123**
Defining a MIB Collection 124
The MIB Poller Summary 125
The MIB Query Tool 130

Reconfiguring EPICenter Ports **131**

Using the EPICenter Debugging Tools **132**

Chapter 10 VoIP and EPICenter-Avaya Integrated Management

Overview **133**

Installation Considerations **134**
TFTP Server Coordination 135

Discovering Avaya Devices **135**

Avaya Devices in EPICenter **136**
Launching the Avaya Device Manager from the Devices Sub-Menu 137

Tools Menu Commands **138**

Launching the Avaya Integrated Management Console from EPICenter **139**

Monitoring IP Phones on Extreme Networks Devices **139**
Importing IP Phones 139
Syncing IP Phones 141
The IP Phones Properties Display 141
IP Phones Reports 142

EPICenter System Properties for Avaya Integration **143**

Launching EPICenter from the Avaya Integrated Management Console **145**

Chapter 11 Policy Manager Overview

Overview of the Policy Manager **147**

Basic EPICenter Policy Definition **148**

Policy Types **149**
Access-based Security Policies 149
IP-Based Policies (Access List Policies) 151
Source Port Policies 154
VLAN Policies 155

Policy Named Components **156**

Policy Access Domain and Scope **159**

Using Groups in Policy Definitions **160**
Precedence Relationships within the Policy Manager 161

Policy Configuration **161**

EPICenter Policy Limitations **162**

Appendix A Troubleshooting

Troubleshooting Aids **165**
Using the Stand-alone Client Application 165
Using the Browser-based Client (Windows Only) 166

EPICenter Client **167**

EPICenter Database **168**

EPICenter Server Issues **169**

VLAN Manager **172**

Alarm System **173**

ESRP Monitor **174**

Inventory Manager **175**

Grouping Manager **176**

Printing **176**

Topology **176**

STP Monitor **177**

Reports **177**

Appendix B EPICenter Utilities

The DevCLI Utility **179**
Using the DevCLI Commands 180
DevCLI Examples 182

Inventory Export Scripts **183**
Using the Inventory Export Scripts 183
Inventory Export Examples 184

The SNMPCLI Utility **185**
Using the SNMPCLI Utility 185
SNMPCLI Examples 186

Port Configuration Utility **187**

The AlarmMgr Utility **188**
Using the AlarmMgr Command 189
AlarmMgr Output 191
AlarmMgr Examples 191

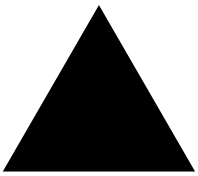
The FindAddr Utility **191**
Using the FindAddr Command 192
FindAddr Output 193
FindAddr Examples 194

The TransferMgr Utility **194**
Using the TransferMgr Command 194
TransferMgr Examples 197

The VlanMgr Utility **198**
Using the VlanMgr Command 198
VlanMgr Output 201
VlanMgr Examples 201

The ImportResources Utility **202**
Using the ImportResources Command 202
ImportResources Examples 203

Index **205**



Preface

This preface provides an overview of this guide, describes guide conventions, and lists other useful publications.

Introduction

This guide provides the required information to use the EPICenter software. It is intended for use by network managers who are responsible for monitoring and managing Local Area Networks, and assumes a basic working knowledge of:

- Local Area Networks (LANs)
- Ethernet concepts
- Ethernet switching and bridging concepts
- Routing concepts
- The Simple Network Management Protocol (SNMP)

NOTE

If the information in the Release Notes shipped with your software differs from the information in this guide, follow the Release Note.

Terminology

When features, functionality, or operation is specific to the Summit, Alpine, or BlackDiamond switch family, the family name is used. Explanations about features and operations that are the same across all Extreme switch product families simply refer to the product as the "Extreme device" or "Extreme switch." Explanations about features that are the same for all devices managed by EPICenter (both Extreme devices and others) are simply refer to "devices."

Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

Table 1: Notice Icons

Icon	Notice Type	Alerts you to...
	Note	Important features or instructions.
	Caution	Risk of unintended consequences or recoverable loss of data.
	Warning	Risk of permanent loss of data.

.

Table 2: Text Conventions

Convention	Description
`Screen displays`	This typeface represents information as it appears on the screen.
`Screen displays bold`	This typeface indicates how you would type a particular command.
The words “enter” and “type”	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”
[Key] names	Key names appear in text in one of two ways. They may be • referred to by their labels, such as “the Return key” or “the Escape key.” • written with brackets, such as [Return] or [Esc]. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). For example: Press [Ctrl]+[Alt]+[Del].
Words in **bold** type	Bold text indicates a button or field name.
Words in *italicized* type	Italics emphasize a point or denote new terms at the place where they are defined in the text.

Related Publications

The EPICenter documentation set includes the following:

- *EPICenter Reference Guide*
- *EPICenter Concepts and Solutions Guide* (this guide)
- *EPICenter Installation and Upgrade Note*
- *EPICenter Release Notes*
- *EPICenter License Agreement*

Both the *EPICenter Reference Guide* and the *EPICenter Concepts and Solutions Guide* can be found online in Adobe Acrobat PDF format in the `docs` subdirectory of the EPICenter installation directory. They are also available in a Microsoft Windows environment from the EPICenter **Start** menu.

You must have Adobe Acrobat Reader version 4.0 or later (available from http://www.adobe.com free of charge) to view these manuals.

The EPICenter software also includes context-sensitive online Help, available from the Help menu in each EPICenter applet, as well as through Help buttons in most windows and dialogs throughout the software.

Other manuals that you will find useful are:

- *ExtremeWare Software User Guide*
- *ExtremeWare Command Reference Guide*
- *ExtremeWare XOS Concepts Guide*
- *ExtremeWare XOS Command Reference Guide*

For documentation on Extreme Networks products, and for general information about Extreme Networks, see the Extreme Networks home page:

- http://www.extremenetworks.com

Customers with a support contract can access the Technical Support pages at:

- http://www.extremenetworks.com/services/eSupport.asp

  The technical support pages provide the latest information on Extreme Networks software products, including the latest Release Notes, information on known problems, downloadable updates or patches as appropriate, and other useful information and resources.

Customers without contracts can access manuals at:

- http://www.extremenetworks.com/services/documentation/

1 EPICenter Overview

This chapter describes:

- The features of the EPICenter™ software
- The EPICenter software components

Introduction

Today's corporate networks commonly encompass hundreds or thousands of systems, including individual end user systems, servers, network devices such as printers, and internetworking systems. Extreme Networks™ recognizes that network managers have different needs, and delivers a suite of ExtremeWare™ management tools to meet those needs.

EPICenter is a powerful yet easy-to-use application suite that facilitates the management of a network of Summit™, BlackDiamond™, and Alpine™ switches, as well as selected third-party switches. EPICenter makes it easier to perform configuration and status monitoring, create virtual LANs (VLANs), and implement policy-based networking in enterprise LANs with Extreme Networks switches. EPICenter offers a comprehensive set of network management tools that are easy to use from a client workstation running EPICenter client software, or from a workstation configured with a web browser and the Java plug-in.

EPICenter leverages the three-tier client/server architecture framework represented by Java applets, and can be accessed using Microsoft Internet Explorer or with Sun's Java Plug-in. The EPICenter application and database support two of the most popular operating environments in the marketplace, Microsoft Windows 2000/XP and Sun Microsystems' Solaris.

EPICenter Features

In large corporate networks, network managers need to manage systems "end to end." The EPICenter software is a powerful, flexible and easy-to-use application for centralizing the management of a network of Extreme switches and selected third-party devices, regardless of the network size. The EPICenter software provides the vital SNMP, HTML, and CLI-based tools you need for network-wide management of Extreme Networks Summit, Black Diamond, and Alpine switches.

- **Network Control**. The EPICenter software provides configuration and monitoring of Extreme Networks' switches and selected third-party devices anywhere on the network simultaneously.

- **Intelligent Management**. Extreme SmartTraps™ (patent pending) automatically gather switch configuration changes and forward them to the EPICenter server, thereby minimizing network management traffic. EPICenter separates its SNMP status polling, used to asses a device's connectivity, from its less frequent and more data-intensive detailed polling.
- **Hierarchical Displays**. Most information, including that found in EPICenter topology maps, VLAN management, configuration management, and real-time statistics, is dynamically presented in an easy-to-navigate hierarchical tree.
- **Multi-platform capability**. The EPICenter server supports Sun SPARC/Solaris and Intel, Windows 2000, and Windows XP. Client applications on either of these platforms can connect to servers on either platform.
- **Support for multiple users with security**. Users must log in to the application, and can be granted different levels of access to the application features based on their assigned role. Three basic predefined roles are provided, and additional user roles can be created. Telnet and SSH access to Extreme Networks switches can also be controlled based on the user identity.
- **Installed or web-based clients**. The EPICenter software gives you a choice of installing full-function client software, or connecting to the EPICenter server through a web-browser-based client, available on Windows client machines. The browser-based client provides slightly limited functionality due to the constraints of the browser environment.
- **Monitor wireless Access Points and wireless clients.** Through EPICenter's dynamic reports you can monitor the status of the Altitude 300 APs connected to your network and monitor wireless client activity connected through those APs. You can also detect rogue APs connected to the network, and add them to a "safe" list, or disable their access if necessary.
- **Manage large numbers of devices.** The EPICenter Gold Upgrade enables the EPICenter server to manage up to 2000 devices with a single installation of the EPICenter software. For even larger networks you can split the management task among several EPICenter servers in a distributed server mode that lets you monitor the status of those servers from a single client.
- **Policy-based Management.** The EPICenter Policy Manager Upgrade is an optional, separately-licensed component of the EPICentersoftware that lets you work with high-level policy components (users, desktop systems, groups of users, devices, or applications) in defining network policies used to protect and guarantee delivery of mission-critical traffic. The policy system translates these into the specific information needed for QoS configuration of network devices. It also detects overlaps and conflicts in policies, with precedence rules for resolving conflicting QoS rules.

Extreme Networks switches and many other MIB-2 compatible devices can be monitored and controlled from a central interface, without exiting EPICenter to run a separate program or telnet session. Features such as SmartTraps (for Extreme Networks devices) and the EPICenter alarm system further maximize network monitoring capability while maintaining network usage efficiency.

All devices in the EPICenter inventory database—both Extreme Networks devices and third-party devices—can also appear on a topology map. The EPICenter alarm system can handle SNMP traps from any device in the inventory database, including RMON traps from devices with RMON enabled. The Real-Time Statistics module can display statistics for any device with RMON enabled, and the IP/MAC Finder applet supports all devices running MIB-2 and the Bridge MIB, with the exception of user mapping, which is specific to Extreme devices.

You can organize your network resources into multiple, overlapping groups (including groups made up of selected ports from multiple switches) that you can manage as a single entity. Device groupings can be based on a variety of factors, such as physical location, logical grouping, devices that support SSH2, and so on. Using device groups, you can search for individual IP addresses and identify their connections into the network. You can monitor the status of your network devices visually through the Inventory Manager or via a Topology map, or by setting alarms that will notify you about conditions or

events on your network devices. You can display an overview of the status of your network devices as a hierarchical topology map.

Access to the features of EPICenter can be restricted based on user roles, so that users with certain roles can have a combination of read-only access, read-write access, or no access to certain features within EPICenter. Feature access can also be allowed or restricted on a server-wide basis, so that no users will have access to selected features of the product.

The EPICenter features are described in somewhat more detail in the following sections. The rest of this manual describes how to best use these features to manage various aspects of your network. For detailed instructions on using specific features of EPICenter see the context-sensitive online Help available via the Help menu at the top of every feature, as well as via Help buttons throughout the user interface of the product. The *EPICenter Reference Guide* also provides a detailed description of the functionality of each EPICenter feature.

Inventory Management

EPICenter's Inventory Manager feature keeps a database of all the devices managed by the EPICenter software. Any EPICenter user with read-only access to this feature can view status information about the switches currently known to the EPICenter database.

The EPICenter Inventory Management provides a discovery function to discover the components of your network. Users with the appropriate access (roles with read/write access) can use this feature to discover Extreme Networks devices as well as any third-party devices running a MIB-2 compatible SNMP agent. Devices may be discovered by specific IP address or within a range of IP addresses. Third-party devices that support SNMP version 3 (SNMPv3) are discovered as SNMP version 1 (SNMPv1) and are added to the EPICenter database as SNMPv1 devices.

Network devices can also be added to the EPICenter database manually, using the Inventory Manager Add function. Once a network device is known to the EPICenter database, you can assign it to a specific device group, and configure it using the VLAN Manager, the Configuration Manager, Telnet macros, or the embedded Device Manager (ExtremeWare Vista for Extreme devices). The Inventory Manger also allows you to set a device to offline status so that EPICenter will not poll and can ignore traps when a device is scheduled for maintenance.

EPICenter also provides a command-line utility that lets you create device groups and import large numbers of devices into the inventory database through scripts, to streamline the process of adding and organizing devices for management purposes. These utilities are described in the Appendix B "EPICenter Utilities".

The Inventory Manager displays detailed information about individual devices through a front panel image that provides a visual device representation, with associated detailed configuration and status information. Any EPICenter user can view status information about the network devices known to the EPICenter database. Users with the appropriate access permissions can also view and modify configuration information for those switches.

The Alarm System

The EPICenter Alarm System provides fault detection and alarm handling for the network devices monitored by the EPICenter software. This includes Extreme devices and some third-party devices—those that the EPICenter software can include in its Inventory database. The Alarm System also lets you define your own alarms that will report errors under conditions you specify, such as

repeated occurrences or exceeding threshold values. You can specify the actions that should be taken when an alarm occurs, and you can enable and disable individual alarms.

Fault detection is based on SNMP traps, RMON traps, Syslog messages, and some limited polling. The Alarm System supports SNMP MIB-2 and the Extreme Networks private MIB. You can also configure alarms based on certain event thresholds, or on the content of Syslog messages. When an alarm occurs you can specify actions such as sending e-mail, forwarding a trap, running a program, running a script, or a Telnet macro, sending a page, or sounding an audible alert.

The Configuration Manager and the Firmware Manager

The EPICenter Configuration Manager provides a mechanism and a graphical interface for uploading and downloading configuration files to and from managed devices. The EPICenter Firmware Manager can download ExtremeWare software images and BootROM images to Extreme Networks devices, or to Extreme modules that include software.

The Configuration Manager provides a framework for storing the configuration files, to allow tracking of multiple versions. Configuration file uploads can be performed on demand, or can be scheduled to occur at regular times—once a day, once a week, or at whatever interval is appropriate.

The Firmware Manger can be configured to automatically track the firmware versions in Extreme Networks devices, will indicate whether newer versions are available, and can automatically retrieve those versions from Extreme Networks if desired.

The Grouping Manager

One of the powerful features of the EPICenter software is its ability to take actions on multiple devices or resources with a single user action. The Grouping Manager facilitates this by letting you organize various resources into hierarchical groups, which can then be referenced in other applets. You can then take actions on a group, rather than having to specify the individual devices or ports that you want to affect.

You can also create or import named resources such as users and workstations, which can be mapped through the Grouping Manager to IP addresses and ports. This capability is especially important in relationship to the optional Policy Manager applet, which takes advantage of these types of resources to simplify the creation of QoS and Access List policies.

The IP/MAC Address Finder

The IP/MAC Address Finder applet lets you search for specific network addresses (MAC or IP addresses) and identify the Extreme Networks switch and port on which the address resides. You can also use the IP/MAC Finder applet to find all addresses on a specific port or set of ports. If you have enabled EPICenter's periodic MAC Address polling, which does polls for edge port address information, you can perform a fast address search by just searching the EPICenter database for this information. ALternatively you can direct EPICenter to search the FDBs of specific Extreme Networks switches. You can export the results of your search to a file, either on the server or on your local (client) system.

The Telnet Feature

The Telnet feature provides two ways to interact with devices via Telnet: either by running an interactive telnet session on a selected device, or by creating Telnet macros (scripts of CLI commands) that can be executed on multiple devices in one operation, and can be executed repeatedly. Results of

the most recent macro run on each device are saved into log files, and can be viewed from within the Telnet applet.

Saved telnet macros can also be run from outside the Telnet applet, through the Tools menu or from the right-click pop-up menus that are available in most EPICenter features. When a macro is created, the administrator can define both an execution context—whether the macro should be available to be run on all devices in a device group, or only individual devices or individual ports— and can allow these macros to be run by users with specific roles.

You can use the interactive Telnet capability (but not telnet macros) to view and modify configuration information for some Cisco and 3COM devices as well as for Extreme Networks devices.

Real-Time Statistics

The Real-Time Statistics feature of the EPICenter software provides a graphical presentation of utilization and error statistics for Extreme switches in real time. The data is taken from Management Information Base (MIB) objects in the etherHistory table of the Remote Monitoring (RMON) MIB. You can choose from a variety of styles of charts and graphs as well as a tabular display.

You can view data for multiple ports on a device, device slot, or within a port group, optionally limiting the display to the "top N" ports (where N is a number you can configure). You can also view limited historical statistics for an individual port. If you choose to view a single port, the display shows the value of the selected variable(s) over time, and can show utilization history, total errors history, or a breakdown of individual errors.

In addition, the Real-Time Statistics applet lets you "snapshot" a graph or table as a separate browser page. You can then save, print, or e-mail the page.

Topology Views

The EPICenter software's Topology feature allows you to view your network (EPICenter-managed devices and the links between Extreme Networks devices) as a set of maps. These maps can be organized as a tree of submaps that allow you to represent your network as a hierarchical system of campuses, buildings, floors, closets, or whatever logical groupings you want.

EPICenter can add device nodes to your topology map automatically as devices are added to EPICenter software's device inventory. The EPICenter software automatically detects and adds links that exist between Extreme Networks devices, and organizes the device nodes into submaps as appropriate. The links between devices provide information about the configuration and status of the links.

You can customize the resulting maps by creating submaps, moving map elements within or between submaps, adding new elements, such as links, "decorative" (non-managed) nodes, and text, and customizing the look and labeling of the discovered nodes themselves. In addition, options are available to organize and optimize the map layout to display very large numbers of devices with the minimum of device and link overlap. You can place a background image behind your map—either one of the images available with EPICenter, or one you provide yourself, such as a building or campus layout.

The Topology applet shows alarm status for individual devices, and propagates that information up the map hierarchy so that from a higher-level map you can tell the what level of alarms have occurred for devices in a submap. The Topology applet also provides information about the VLANs configured on devices in a topology view. Using the Display VLANs feature, you can visually see which links and devices are configured for a selected VLAN, or select a specific device or link to see what VLANs are configured on that device. You can also configure a VLAN in a topology by adding ports or trunk links.

Finally, from a managed device node on the map, you can invoke other EPICenter functions such as the alarm browser, telnet, real-time statistics, a front panel view, the VLAN Manager, or ExtremeWare Vista for the selected device.

Enterprise-wide VLAN Management

A virtual LAN (VLAN) is a group of location- and topology-independent devices that communicate as if they were on the same physical local area network (LAN).

The EPICenter VLAN Manager is an enterprise-wide application that manages many aspects of VLANs on Extreme Network's Summit, BlackDiamond, and Alpine switches. Any EPICenter user can view status information about the VLANs known to EPICenter across the network. Users with the appropriate access can create and delete VLANs, add and remove ports from existing VLANs, and create and modify the protocol filters used to filter VLAN traffic. When creating or modifying a VLAN, you can get EPICenter to determine whether there is connectivity between the devices you have included in the VLAN, and if not, it can recommend what ports and devices you should add to achieve connectivity.

The ESRP Manager

The Extreme Standby Router Protocol (ESRP) is a feature of ExtremeWare that allows multiple switches to provide redundant layer 3 routing services, as well as layer 2 redundancy, to users. The ESRP Manager displays the status of ESRP-enabled VLANs and the ESRP-enabled switches in those VLANs. You can view a summary status for all the ESRP-enabled VLANs being monitored by the EPICenter software. You can also view detailed information for an individual ESRP-enabled VLAN and the switches in those VLANs.

The STP Monitor

The EPICenter Spanning Tree Protocol (STP) Monitor module displays information about STP domains network-wide at the domain, VLAN, device, and port levels. The STP Monitor can monitor STP domains configured on devices running ExtremeWare 6.2.2 or later. Earlier versions of ExtremeWare supported the Spanning Tree protocol, but STP information via SNMP (required for EPICenter) is available only with ExtremeWare version 6.2.2 or later.

EPICenter Reports

EPICenter Reports are HTML pages that can be accessed separately from the main EPICenter user interface, without logging in to the full EPICenter client. EPICenter reports do not require Java, so reports can be loaded quickly, even over a dial-up connection, and can be viewed on systems that cannot run the browser-based or installed EPICenter clients. Reports can be printed using the browser print function.

The Reports capability provides a large number of predefined HTML reports that present a variety of types of information from the EPICenter database. You can also create your own reports by writing Tcl scripts. Further, within the Reports Module are several useful tools such as a MIB Browser and other tools that can provide EPICenter system information.

The Reports module can also be accessed from the Navigation toolbar within the EPICenter client application. A Summary report is displayed on the EPICenter Home page that provides basic information on the status of EPICenter devices and alarms. From this report you can access other more detailed reports.

Role-based Access Management

All EPICenter users must log in with a user name and password in order to access EPICenter features. EPICenter initially provides four user roles:

- Monitor role—users who can view status information only.
- Manager role—users who can modify device parameters as well as view status information.
- Administrator role—users who can create, modify and delete EPICenter user accounts as well as perform all the functions of a user with Manager access.
- Disabled role—users whose account information is maintained, but who have no access to any features of the product.

An Administrator user can create additional roles, can modify the capabilities available under each role, and can add and delete EPICenter users, as well as enable or disable access for individual users.

Through the EPICenter Admin applet, EPICenter can be configured to act as a Remote Authentication Dial In User Service (RADIUS) server. It can then be contacted by RADIUS clients (such as Extreme Networks switches) to configure access permissions for Extreme switches, and to authenticate user names and passwords. The use of EPICenter as a RADIUS server avoids the need to maintain user names, passwords, and access permissions in each switch, and instead centralizes the configuration in one location in EPICenter.

As an alternative, EPICenter can be configured as a RADIUS client, or RADIUS authentication functionality can be disabled.

EPICenter Stand-alone Utilities

The EPICenter software provides a number of stand-alone utilities or scripts that streamline the process of getting information into and out of the EPICenter database, or facilitate certain device troubleshooting functions. These include the following:

- The DevCLI utility lets you add devices to and remove devices from the EPICenter inventory database via command, and supports batch additions and deletions specified via a file.
- A set of Inventory Export scripts that enable you to export information from the EPICenter database about the devices that are being managed. The information is provided in a format suitable for import into other applications, such as a spreadsheet.
- The SNMPCLI utility provides SNMP Get, GetNext, and SNMP walk features that may be needed to obtain device MIB information for troubleshooting.
- A set of utilities that provide a command line interface to several EPICenter software functions. These include the AlarmMgr utility, FindAddr utility, TransferMgr utility, and VlanMgr utility. These utilities enable you to perform certain EPICenter functions from the command line (or through a script) rather than through the EPICenter graphical user interface. Results from the Alarm Manager utility and the Find Address utility can be output to a file.

The EPICenter Policy Manager Upgrade

The EPICenter Policy Manager is a separately-licensed component of the EPICenter product family. When a Policy Manager license is installed on the EPICenter server, the Policy and Voice over IP icons icon appears in the Navigation Toolbar at the left of your browser window. When you purchase the optional Policy Manager, you will receive a separate license key for that feature.

The Policy Manager includes three modules:

- The Policies View, where you can create, view, and modify EPICenter policy definitions for Extreme Networks devices.
- The ACL Viewer, where you can view the access list and QoS rules generated by the Policy Manager for the devices in your network.
- The Voice over IP Manager module, where you can configure quality of service parameters for VLANs that are used to carry Voice over IP traffic. (This is a separate feature unrelated to the features available for IP phone management available through EPICenter integration with the Avaya Integrated Management software.

Distributed Server Mode (EPICenter Gold Upgrade)

To manage very large numbers of network devices, or devices that are geographically distributed, the management task can be divided up between multiple EPICenter servers. Each server in the server group is updated at regular intervals with network summary and status information from the other servers in the group. From the EPICenter home page, a client attached to any one of the servers in the server group can view summary status information from the other servers in the group in addition to the standard Network Summary report. The EPICenter client also lets the user easily navigate between the different servers in the group to see detailed management information about the devices managed by those servers.

EPICenter Software Architecture

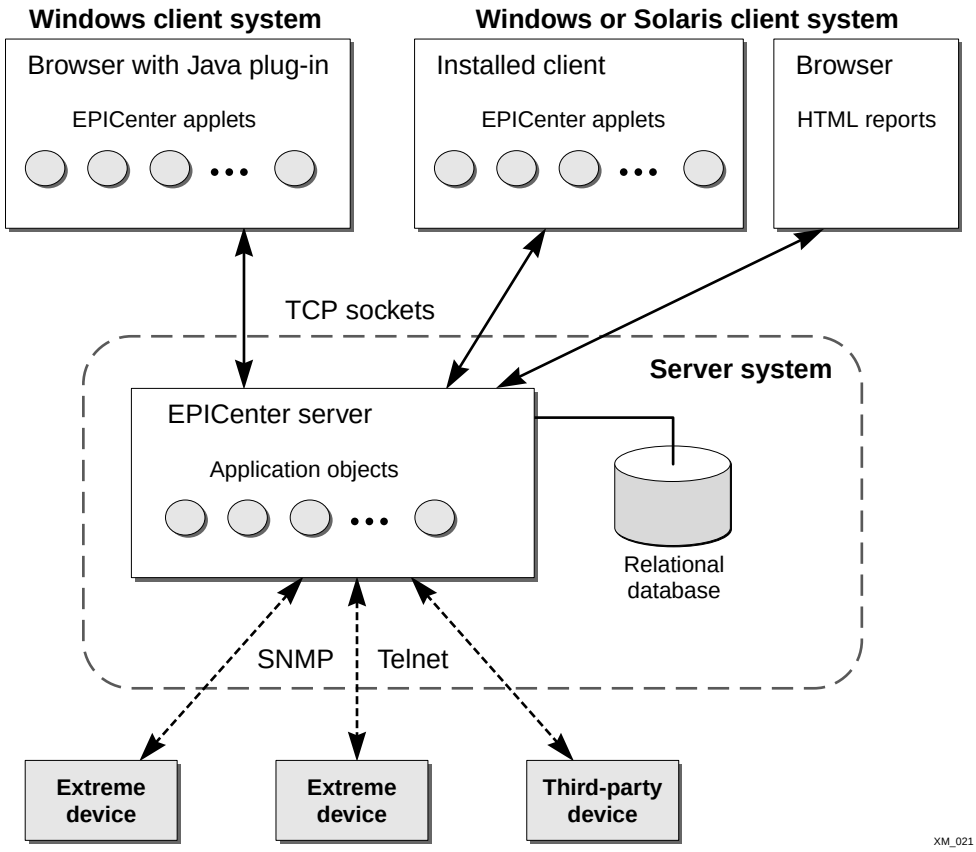
The EPICenter software is made up of three major functional components:

- The EPICenter Server, which is based on the Tomcat Java server. The server is responsible for downloading applets, running servlets, managing security, and communicating with the database.
- A Relational Database Management System (RDBMS), Sybase Adaptive Server Anywhere, which is used as both a persistent data store and a data cache.
- EPICenter client applications. This can be an installed client application that runs on a Windows 2000, Windows XP, Windows 2003 Server, or a Solaris system.

  On Windows systems, the client can also be a set of Java applets downloaded on demand from the server into the Microsoft Internet Explorer 6.0 browser running the Java plug-in (version 1.4.2_05).

Figure 1 illustrates the architecture of the EPICenter software.

Figure 1: EPICenter software architecture



Extreme Networks Switch Management

The EPICenter software primarily uses the Simple Network Management Protocol (SNMP) to monitor and manage the devices in the network. The EPICenter server does an status poll, by default every five minutes, of all the devices it is managing to determine if the devices are still accessible. It also does a full detailed poll of each device at longer intervals. This interval for this less frequent detailed polling can be adjusted on each individual device. The EPICenter software also gives you the ability to gather device status at any time using the **Sync** feature in the Inventory Manager applet.

To avoid the overhead of frequent device polling, the EPICenter software also uses a mechanism called SmartTraps to identify changes in Extreme Networks device configuration. In addition, standard SNMP MIB-2 traps can be used to define alarms for a large variety of other conditions.

SNMP and MIBs

EPICenter uses SNMP whenever possible to obtain information about the devices it is managing, and to implement the configuration changes made through EPICenter features.

The Remote Monitoring (RMON) MIB

EPICenter can use statistics gathered from the Remote Monitoring (RMON) MIB to provide utilization statistics on a port-by-port basis, if RMON is supported and enabled on the Extreme Networks devices EPICenter is managing. Utilization and error statistics can be displayed within the Real-Time Statistics applet, which provides a number of chart, graph, and tabular display formats. RMON utilization statistics can also be displayed as end-point annotations on the links between devices on a Topology map. The EPICenter Alarm Manager also provides the ability to define threshold-based RMON rules for generating trap events that can be used in EPICenter alarm definitions.

Traps and Smart Traps

Fault detection is based on Simple Network Management Protocol (SNMP) traps, syslog messages, and some limited polling. The Alarm System supports SNMP Management Information Base-2 (MIB-2), the Extreme Networks private MIB, Remote Monitoring (RMON) traps, and selected traps from other MIBs. The EPICenter software uses a mechanism called SmartTraps to identify changes in Extreme Networks device configuration.

When an Extreme Networks switch is added to the EPICenter database, the EPICenter software creates a set of SmartTraps rules that define the configuration change events that the EPICenter server needs to know about. These rules are downloaded into the Extreme Networks switch, and the EPICenter server is automatically registered as a trap receiver on the switch. Subsequently, whenever a status or configuration change takes place, the ExtremeWare software in the switch uses the SmartTraps rules to determine if the EPICenter server should be notified. These changes can be changes in device status, such as fan failure or overheating, or configuration changes made on the switch through the ExtremeWare CLI or ExtremeWare Vista.

For non-Extreme devices, EPICenter does not automatically register itself as a trap receiver; you must manually configure those devices to send traps to EPICenter. See Appendix B in the *EPICenter Reference Guide* for information on configuring devices to send traps to EPICenter.

Device Status Polling

EPICenter uses several types of polling to monitor the status of the devices it manages. Since device polling adds a certain amount of traffic load to the network, EPICenter tries to minimize the amount of polling that it does, and many aspects of its polling algorithms are configurable.

EPICenter polls for basic device status approximately every five minutes using SNMP. This poll interval can be changed in the Administration applet under the Server Properties for SNMP. EPICenter also polls periodically for detailed device status information. By default, this interval is 30 minutes for Extreme Networks modular chassis switches, and 90 minutes for Extreme Networks stackable chassis switches. The detailed polling interval can be set for individual devices through the Inventory Manager feature. The detailed polling gets more complete information, still only polls for information that has changed; a manual sync is required to retrieve all information about the device. A sync is performed automatically whenever the EPICenter client is started.

Telnet Polling

When it is not possible to use SNMP to obtain information from Extreme Networks devices, EPICenter will use Telnet polling instead. EPICenter uses Telnet polling to obtain MAC address information for edge ports from a device Forwarding Database (FDB) and to obtain netlogin information. For some old versions of ExtremeWare, ESRP information must be obtained via Telnet rather than SNMP. Telnet polling is also used to obtain power supply IDs for Alpine devices.

You can disable Telnet polling if necessary through the Server Properties for Devices in the Admin applet. However, you will lose the ability to collect edge port information via FDB polling, as well as netlogin information.

Edge Port Polling Using the MAC Address Poller

EPICenter can maintain information about the MAC and IP addresses detected on Extreme Networks switch edge ports by polling the FDB tables of the Extreme switches it is managing. If MAC address polling is enabled, EPICenter uses Telnet polling to retrieve FDB information at regular intervals based on the settings of server properties in the Administration applet.

MAC address polling can be enabled or disabled globally. If enabled, it can then be disabled for individual devices or for specific ports on devices.

EPICenter distinguishes edge ports from trunk ports based on whether the port is running the Extreme Discovery Protocol (EDP). EPICenter assumes that ports that run EDP are trunk ports, and ports that do not run EDP are edge ports. However, since non-Extreme devices do not run EDP, EPICenter may mis-identify trunk ports to third party devices as edge ports. You can disable MAC address polling on individual ports to prevent EPICenter from polling trunk ports for MAC addresses.

Syncing Device Status with the EPICenter Database

A user with an appropriate role (a role with read/write access to the Inventory Manager) can use the **Sync** command from the Inventory Manager to update the device status in the EPICenter database when the users believes that the device configuration or status is not correctly reported in EPICenter applets. **Sync** causes EPICenter to poll the switch and update *all* configuration and status information except for uploaded configuration files. During a **Sync** operation the SmartTraps rules are also reset in case the user has accidentally deleted the trap receiver or any SmartTrap rules.

Extreme Networks Device Support

Extreme Networks devices running the ExtremeWare software version 2.0 or later, are supported by most features in the EPICenter system, including the VLAN Manager and the graphical display features of the Inventory Manager applet. Some features, such as ESRP, or the Policy Manager, require more recent versions of the ExtremeWare software. See the *EPICenter Release Note* for specific information about the hardware and software versions supported by this release of the EPICenter software.

Third-Party Device Support

Any device running a MIB-2 compatible SNMP agent can be discovered by the EPICenter Inventory manager, and saved in the Inventory database. All devices in the database can also appear on a topology map. The EPICenter alarm system can handle SNMP traps from any device in the inventory database, including RMON traps from devices with RMON enabled. The Real-Time Statistics module can display statistics for any device with RMON enabled, the IP/MAC Finder applet supports all devices running MIB-2 and the Bridge MIB, with the exception of user mapping, which is specific to Extreme devices.

In the Telnet applet, you can use the Telnet feature with any device that supports a Telnet interface. In the Inventory Manager, all Extreme devices and selected third-party devices (including certain Cisco and 3COM devices) can display a device-specific front panel view, and a rear panel view if appropriate. In addition, vendor-specific generic images are available for additional devices, such as Sun and Nortel, and a standard generic image can be displayed for all other “unknown” MIB-2 compatible devices. New

device images and configuration description files may be added over time—check the Extreme Networks web site for information on new device support.

EPICenter also provides support for Avaya Voice network devices through an integration of EPICenter and Avaya Integrated Management software that is co-resident on the same system.

2 Getting Started with EPICenter

This chapter covers how to use some of the basic features of the EPICenter system:

- Starting EPICenter.
- How to get Help.
- EPICenter User Roles.
- Creating the Device Inventory.
- Organizing your network elements using groups.
- Using the Alarm System.
- Organizing views of your network using the Topology function.
- Using Basic Reports.

Starting EPICenter

The EPICenter software consists of a server component that runs on a Windows or Solaris server, and a client component, that can be installed and run on separate Windows or Solaris systems.

Once the EPICenter server is running, multiple clients can connect to it. The EPICenter software supports multiple administrator users, with different roles that determine the EPICenter functions each user can perform.

This chapter assumes you have successfully installed (or upgraded to) the current EPICenter software version—version 5.0 or later, and that the EPICenter server is running.

If you have not yet installed version 5.0, see the *EPICenter Installation and Upgrade Note* for instructions. The *Installation and Upgrade Note* is included in the EPICenter product package along with the EPICenter software CD, and is also available in Adobe PDF format on the CD, and from the Extreme Networks web site.

Starting the EPICenter Server

The EPICenter Server consists of two components:

- The EPICenter Database Server
- The EPICenter Server

Both components must be running in order to run the EPICenter client applets.

In a Windows environment (Windows 2000, XP, or 2003 Server), the recommended (and default) method of installing the EPICenter server components is as services. If you have installed the EPICenter components as services, the two EPICenter Server components will start automatically when you boot the server.

If you have not installed EPICenter as services, or if you have installed EPICenter in a Solaris environment, you will need to start the EPICenter server manually.

Starting the EPICenter Server in a Windows Environment

If you installed EPICenter as a regular application rather than as services, you must start the server from the **Start** menu:

1. From the **Start** menu, highlight **Programs**, then **Extreme Networks**, followed by **EPICenter 5.0** to display the EPICenter menu.
2. Click **Start EPICenter 5.0 Server.** This runs `runserv.exe`, a program that starts the two components in the required order.

An MS-DOS window may very briefly appear as these processes are started.

Starting the EPICenter Server in a Solaris Environment

To start the EPICenter server as a daemon (recommended):

```
/etc/init.d/EPICenter start
```

To run the EPICenter Server as an application:

1. Set the current directory to the EPICenter install directory:

   `cd <install_dir>`

   `<install_dir>` is the directory (path) where you installed the EPICenter components. If you installed in the default directory, the path is `/opt/extreme/epc5_0`.

2. Execute **`runserv`** to start the two EPICenter components in the required order.

   ```
   runserv &
   ```

Starting the EPICenter Client

On Windows 2000, Windows XP, or Windows 2003 Server systems, the EPICenter software provides two options for connecting to an EPICenter server from a client system:

- A stand-alone client application. This is the recommended client option.
- A browser-based client you can run from Microsoft Internet Explorer. This client provides slightly limited functionality due to the constraints of the browser environment (for example, you cannot use cut and paste, you cannot save Telnet macros you create, and you cannot use the configuration file viewer or difference viewer).

On Solaris-based systems, only the stand-alone client is supported.

The stand-alone client is installed along with the EPICenter server on the system where the server resides. The stand-alone client can also be installed by itself on any system you want to use as an EPICenter client. See the *EPICenter Installation and Upgrade Note* for instructions on installing the client on a system without the EPICenter server.

For Windows 2000, Windows XP, or Windows 2003 Server, the browser-based client is a Java applet that is downloaded from the EPICenter server when you run it, and requires the following software on the client:

- Internet Explorer 6.0 with the Java Plug-in version 1.4.2_05 or later.

Starting the EPICenter Client in a Windows Environment

To start the EPICenter stand-alone client:

1. From the **Start** menu, highlight **Programs**, then **Extreme Networks**.
2. If you are running the client on the system where the EPICenter server is installed, select **EPICenter 5.0**, then select **EPICenter 5.0 Client**

   If you are running the client on a system *different* from where the EPICenter server is installed, select **EPICenter 5.0 Client**, then select **Client Application.**

   The EPICenter Client Login window appears, as shown in Figure 3 on page 29.

To start the EPICenter client in a browser window:

1. Launch your web browser.
2. Enter the following URL:

   `http://<host>:<port>/`

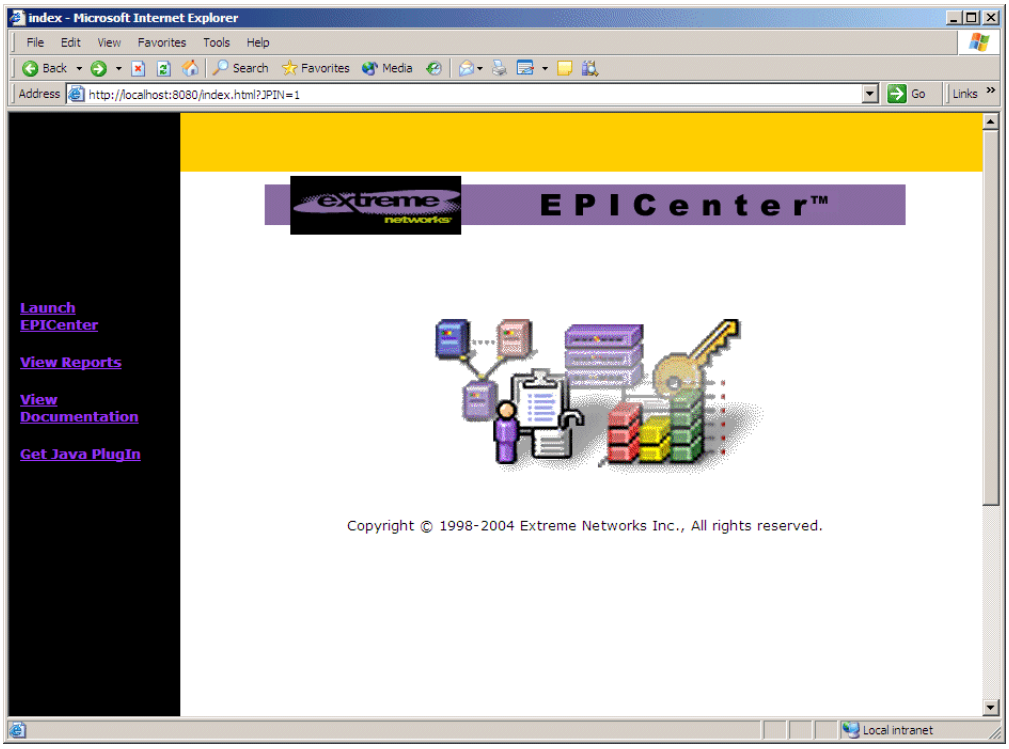
   In the URL, replace *<host>* with the name of the system where the EPICenter server is running. Replace *<port>* with the TCP port number that you assigned to the EPICenter Web Server during installation.

   NOTE

   If you configured your EPICenter server uses the default web server port, 80, you do not need to include the port number.

   The EPICenter browser-based client first presents a start-up page, as shown in Figure 2.

Figure 2: EPICenter Start-up page



3 In the left-hand column, click the **Launch EPICenter** link to display the EPICenter login page.

Starting the EPICenter Client in a Solaris Environment

To start the EPICenter client in a Solaris environment:

1 Set the current directory:

```
cd <install_dir>
```

<install_dir> is the directory (path) where you installed the EPICenter components. If you installed in the default directory, the path is `/opt/extreme/epc5_0`.

2 Execute the command **`runclient`**

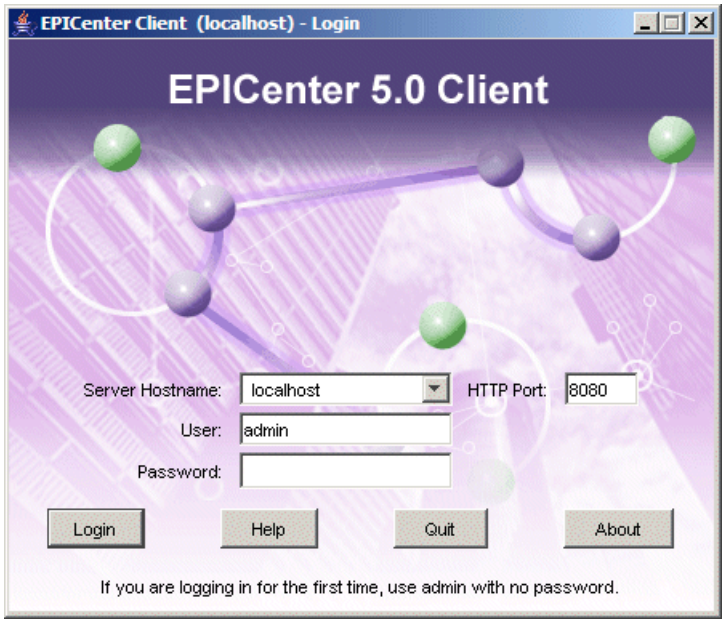
```
runclient &
```

Only the stand-alone client is supported in a Solaris environment.

The EPICenter Client Login Window

The EPICenter installed client starts by opening a Client Login window, as shown in Figure 3.

Figure 3: EPICenter client Login window



The browser-based client also presents a login page, but as you have already provided the server host name in the URL, the browser login window does not ask again for that information.

1 In the installed client login window, type or select in the **Server Hostname** field the name or IP address of the EPICenter server you want to connect to. If you are running the client on a system where an EPICenter server is installed, that server name will appear by default in the Server Hostname field.

2 Type the HTTP port to use to connect to the server in the **HTTP Port** field. The default is port 8080. The port must match the HTTP port configured for the EPICenter server.

3 For either the installed client or a browser-based client, type your EPICenter user name in the **User** field.

- If you are the network administrator logging in to the EPICenter server for the first time since it has been installed, use the name "admin."

  Once you have logged in you will be able to change the administrator password (*strongly recommended*) and create additional user accounts.

- If you are a new user without your own account on the EPICenter server, type "user" as the **User Name**. You will be able to view information in the various modules, but will not be able to change any configurations.

4 Type your password in the **Password** field.

  The default names ("user" and "admin") initially have no password, so you can leave the password field blank.

5 Click **Login**.

  If you are using an evaluation copy of the EPICenter, a dialog box appears informing you that you are using a limited-time license. Click **OK** to acknowledge this.

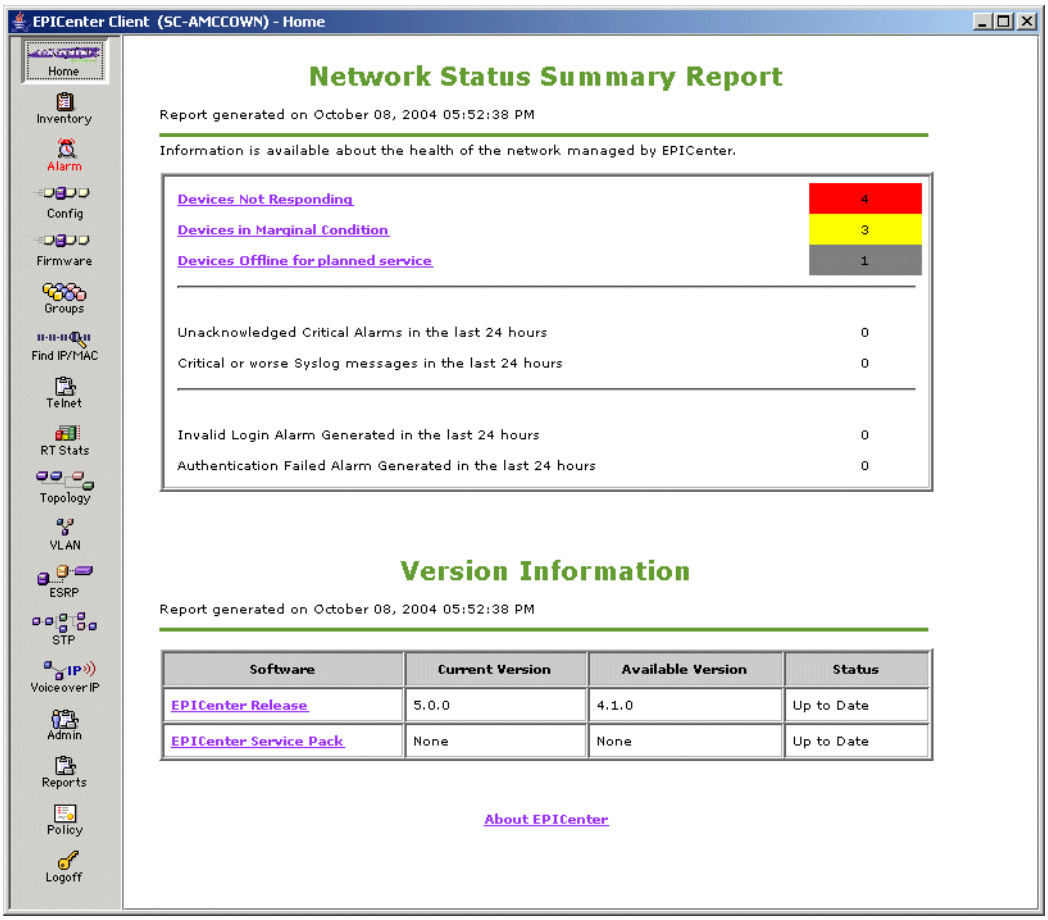
  If you installed EPICenter in non-intrusive mode (so that EPICenter will *not* automatically be registered as a trap receiver on Extreme Networks devices) a message appears reminding you that

you are running in non-intrusive mode. Click **OK** to dismiss this message. See the *EPICenter Installation and Upgrade Note* for more information about non-intrusive mode.

If you enabled Automatic Information Updates when you installed EPICenter, you may be presented with a message indicating that software updates are available. You can click Update Now (which opens the Display Software Images Updates window) or Remind Me Later, which closes the window.

The EPICenter Home page appears, displaying the **Network Summary Report**, as shown in Figure 4.

Figure 4: The EPICenter Home page.


EPICenter Client (SC-AMCCOWN) - Home
Home
Inventory
Alarm
Config
Firmware
Groups
Find IP/MAC
Telnet
RT Stats
Topology
VLAN
ESRP
STP
Voice over IP
Admin
Reports
Policy
Logoff
Network Status Summary Report
Report generated on October 08, 2004 05:52:38 PM
Information is available about the health of the network managed by EPICenter.
Devices Not Responding 4
Devices in Marginal Condition 3
Devices Offline for planned service 1
Unacknowledged Critical Alarms in the last 24 hours 0
Critical or worse Syslog messages in the last 24 hours 0
Invalid Login Alarm Generated in the last 24 hours 0
Authentication Failed Alarm Generated in the last 24 hours 0
Version Information
Report generated on October 08, 2004 05:52:38 PM
Software | Current Version | Available Version | Status
EPICenter Release | 5.0.0 | 4.1.0 | Up to Date
EPICenter Service Pack | None | None | Up to Date
About EPICenter

See "The Network Status Summary Report Page" in Chapter 16 of the *EPICenter Reference Guide* for an explanation of this report.

Getting Help

This guide provides an overview of the EPICenter software features with the goal of showing how you can use EPICenter to simplify your network management tasks and help you solve problems with your network or its devices. It does not provide a detailed explanation of how to use the features of the software.

For detailed help on specific features or applets, EPICenter provides context-sensitive online Help, accessible through **Help** buttons in most EPICenter applets, and through the **Help** menu located in the menu bar at the top of the main window in the EPICenter applets. From the Help menu or Help buttons you can view HTML-based help on the feature you are using, presented in a browser window.

In the Reports feature, there is a **Help** link in the introductory paragraph on the Main reports page.

From the Help menu, the EPICenter Help selection displays the table of contents for the complete Help system.

EPICenter also provides the *EPICenter Reference Guide* which also describes how to use the EPICenter features.

- On Windows-based systems, the *EPICenter Reference Guide* is available in PDF format from the **EPICenter 5.0** menu accessed from the Windows **Start** menu.
- On both Windows and Solaris systems, it can be accessed from the `doc` subdirectory under the EPICenter installation directory. In the Windows environment this is `\Program Files\Extreme Networks\EPICenter 5.0\doc`. In a Solaris environment this is `/opt/extreme/epc5_0/doc`.
- It can be downloaded from the Extreme Networks web site at http://www.extremenetworks.com, under the Support area.

You must have a version of Adobe Acrobat Reader installed (version 4 or later) to view the PDF file. (Acrobat Reader is available for download from Adobe Systems at http://www.adobe.com.

Working with the EPICenter Features

EPICenter is structured as a set of independent Java-based applets that operate on device configuration and status information stored in the EPICenter database. The devices being managed are the common thread between these applets or features, and most applets provide a list of devices managed by EPICenter from which you can choose devices of interest.

EPICenter also supports the grouping of devices into Device Groups. A device group is a set of network devices that have something in common, and that can be managed as a group. Device groups are user-defined, and can be based on any criteria that make sense in your network environment, such as all the devices of a certain type (for example, all wireless switches) or in a certain location. Some functions within EPICenter can be performed on Device Groups, making it easier to perform specific tasks across multiple devices.

Within an applet, the actual functions or operations are initiated by either function buttons, menu items, or both. EPICenter provides several standard menus for functions that are common to all the product features, such as logging off or accessing online Help. In addition, many features provide pop-up menus, accessed by selecting an element such as a device, device group, slot or port, and then clicking the right mouse button to display a pop-up menu. These pop-up menu provide a quick way to view the properties of the selected element, or to perform specific functions for the selected item. The online Help provided in the EPICenter product describes the commands that are available in the various EPICenter features.

Device Selection Persistence

Navigating between EPICenter features is normally done by clicking a button in the Navigation Toolbar, which exits the feature you are currently in (typically abandoning any pending actions) and opens the

new feature in the Main window of the EPICenter product. If a device was selected in the previous feature, that same device will be preselected in the newly-opened feature.

For example, if you select a device in the Inventory Manager, and then run the Alarm Manager, the Alarm Log browser will automatically filter the alarm log to display just the alarms for the device that was selected in the Inventory Manager. If you select a specific alarm entry in the Alarm Log Browser and then run the Topology applet, EPICenter will display the map or sub-map that shows the device on which the selected alarm occurred, with the device selected on the map. (If the device appears on more than one map, EPICenter will let you select which instance you want to see).

Running Features in Separate Windows

In addition to running EPICenter applets from the Navigation Toolbar, certain applets (the Alarm Log Browser, Inventory Manager, Interactive Telnet, VLAN Manager, and Real-Time Statistics) can be run in a separate window to show information about a selected device without leaving the feature you are currently using. This allows you to view status or configuration information about a selected device without losing your place in the feature you are currently working in. The functionality of the applet when it runs in a separate window is somewhat more limited than the features available when the feature is run in its normal mode.

EPICenter User Roles

EPICenter provides four pre-defined roles for levels of user access to the features of the product:

- The Administrator role provided full read/write access to all features of the product, including to the Administration applet where the features of EPICenter itself can be configured, and where users can be added or deleted, and their roles modified.
- The Manager role provided full read/write access to all features of the product except for the Administration applet.
- The Monitor role provided read-only access to the features of the product—a user with a Monitor role could view status and configuration information, but could not do any configuration tasks.
- The Disabled role provides no access to any features of the product.

Every user created in EPICenter is assigned a role which determines the access that user has to the features of the product.

In EPICenter 5.0, the administrator can also create additional roles with any combination of read-only, read-write, or disabled access to different EPICenter product features. In addition, for the Administrator, Manager, and Monitor roles, access can be disabled on a feature-by-feature basis (except that access to the Administration feature is never disabled for the Administrator role).

A user's role determines which features the user can access (if access is disabled, the button for the feature removed from the Navigation Toolbar, with the exception of Telnet, which is greyed out) and what the user can do within the applets to which he has access. A user who's role provides read-write access to a feature can perform all the functions within that feature -- both those that show status information, and those that perform configuration operations, for example. A user who's role provides read-only access will be able to view status and configuration information, but will not be able to perform configuration operations or store information in the EPICenter database.

Roles also used to determine whether a particular user can execute Telnet macros from the Tools menu or from right-click pop-up menu. When a telnet macro is created, one of its attributes is the selection of

roles which can execute the macro. This allows you to create predefined configuration scripts for devices or groups and devices, and control which users can execute those scripts.

Creating the Device Inventory

The first step in using EPICenter is to collect information about the devices on the network to populate the EPICenter inventory database. EPICenter provides a discovery function that can automatically find and retrieve information about the devices on your network. You can also add devices individually. Both of these functions are performed through the Inventory Manager applet.

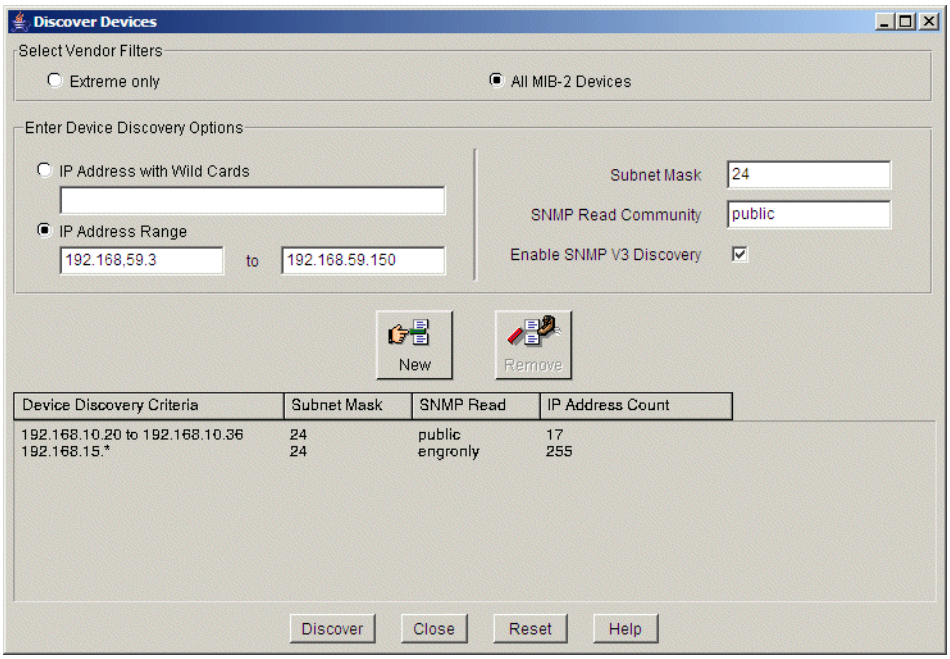
Using Discovery

When you first run EPICenter, the device inventory is empty. The easiest way to populate the inventory database is to use Discovery to automatically detect the devices on your network. With Discovery you can:

- Search for devices by specific IP addresses or ranges of IP address, including using wildcard search parameters to specify the IP address sets you want to query.
- Limit your search to Extreme Networks devices only, or include all discovered MIB-2 devices regardless of manufacturer
- Specify a subnet mask to use for limiting device ranges
- Enable the discovery to use SNMPv3 in its search

Figure 5 shows an example of a discovery specification. You can add multiple address range specifications to be executed in a single discovery operation.

Figure 5: Discovering devices to add to the EPICenter inventory database

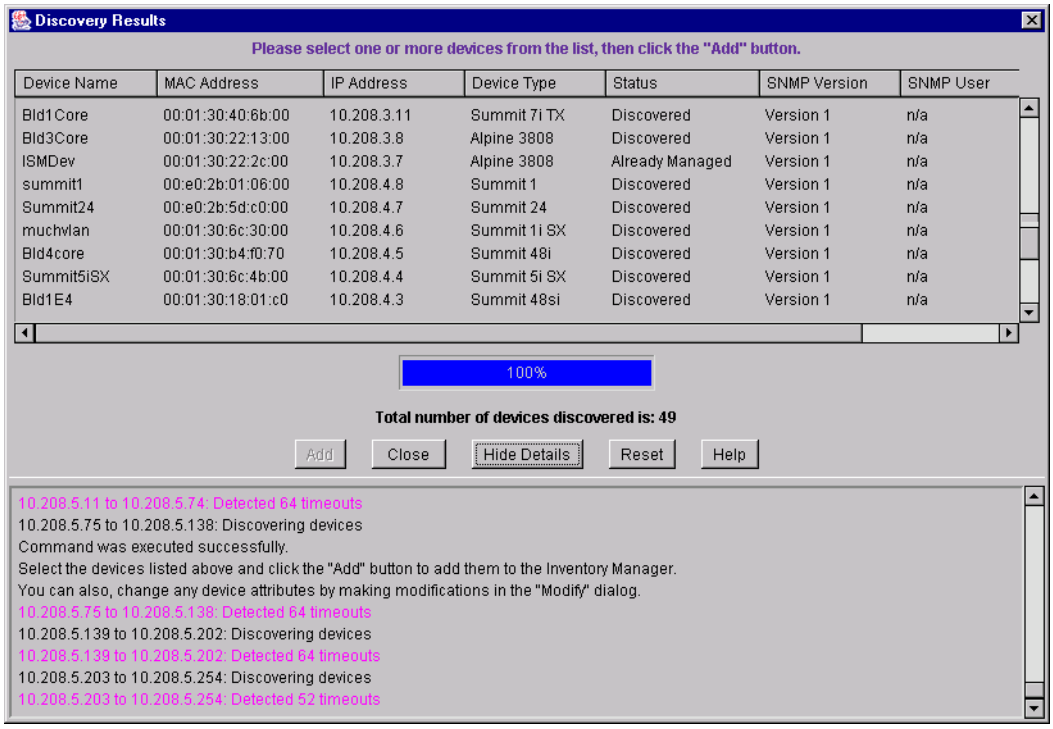


Note that you must provide the SNMP read community string to enable EPICenter to get information from the devices it finds. If your devices do not all use the same read community string, you will need to add each set of devices as a separate specification, as shown in the example.

When you run the discovery, EPICenter returns a list of all the devices it has found within the parameters you provided, as shown in Figure 6.

It **does not** automatically add these devices to the EPICenter inventory; you must select and add the devices either individually or in groups.

Figure 6: Results of a discovery


Discovery Results
Please select one or more devices from the list, then click the "Add" button.
Device Name | MAC Address | IP Address | Device Type | Status | SNMP Version | SNMP User
Bld1Core | 00:01:30:40:6b:00 | 10.208.3.11 | Summit 7i TX | Discovered | Version 1 | n/a
Bld3Core | 00:01:30:22:13:00 | 10.208.3.8 | Alpine 3808 | Discovered | Version 1 | n/a
ISMDev | 00:01:30:22:2c:00 | 10.208.3.7 | Alpine 3808 | Already Managed | Version 1 | n/a
summit1 | 00:e0:2b:01:06:00 | 10.208.4.8 | Summit 1 | Discovered | Version 1 | n/a
Summit24 | 00:e0:2b:5d:c0:00 | 10.208.4.7 | Summit 24 | Discovered | Version 1 | n/a
muchvlan | 00:01:30:6c:30:00 | 10.208.4.6 | Summit 1i SX | Discovered | Version 1 | n/a
Bld4core | 00:01:30:b4:f0:70 | 10.208.4.5 | Summit 48i | Discovered | Version 1 | n/a
Summit5iSX | 00:01:30:6c:4b:00 | 10.208.4.4 | Summit 5i SX | Discovered | Version 1 | n/a
Bld1E4 | 00:01:30:18:01:c0 | 10.208.4.3 | Summit 48si | Discovered | Version 1 | n/a
100%
Total number of devices discovered is: 49
Add
Close
Hide Details
Reset
Help
10.208.5.11 to 10.208.5.74: Detected 64 timeouts
10.208.5.75 to 10.208.5.138: Discovering devices
Command was executed successfully.
Select the devices listed above and click the "Add" button to add them to the Inventory Manager.
You can also, change any device attributes by making modifications in the "Modify" dialog.
10.208.5.75 to 10.208.5.138: Detected 64 timeouts
10.208.5.139 to 10.208.5.202: Discovering devices
10.208.5.139 to 10.208.5.202: Detected 64 timeouts
10.208.5.203 to 10.208.5.254: Discovering devices
10.208.5.203 to 10.208.5.254: Detected 52 timeouts

To add devices to the database, select the set of devices you want to add and click the **Add** button.

For each device or set of devices you add to the inventory database, EPICenter first asks you to provide contact information for those devices:

- The device login name and password
- The EPICenter Device Group in which the device should be place
- The SNMP write community string (for SNMP v1 devices)
- The User Name, Privacy and Authentication protocols and passwords for SNMP V3 devices

EPICenter pops up a dialog box where you can provide this information. It pre-fills the fields with a default set of communication information that you can change as appropriate to the specific devices you are adding.

The information you provide in the pop-up dialog is used for *all* the devices in the set you have selected to add. Therefore, if you have devices that use different passwords, protocols, or community strings, you must add them to the database in separate Add operations.

Adding Devices Individually

There may be a number of situations in which you want to add an individual device to the inventory database without doing a discovery. In this case you can use the Add Device function to add a device to the inventory. Click the **Add** button at the top of the page to bring up the **Add Devices and Device Groups** dialog with the **Device** tab displayed.

You must input the IP address of the device you want to add, as well as the communication information for the device. EPICenter pre-fills the fields in the Add dialog with the default communication information—you can change it as appropriate.

Setting up Default Device Contact Information

For simplicity in managing multiple devices in large networks, administrators typically use the same logins, passwords, community strings and so on, for multiple devices. Therefore, to save time when adding new devices, EPICenter provides default values for these communication parameters.

To save time when you add your own network devices to the EPICenter inventory, you can configure the default values to those used in your own network.

To change the default communication values, click the **Default** button at the top of the Inventory Manager main page.

EPICenter uses the Extreme Networks default values for its switches as the defaults in EPICenter:

- Login as *admin* with no password
- SSH2 disabled
- For Cisco devices only, the default Cisco enable password (none)
- Default SNMP v1 community strings *public* (for read) and *private* (for write)
- SNMP V3 user *initialmd5*
- SNMP V3 privacy set to **No Privacy**, with no password
- SNMP V3 authentication set to **MD5 Authentication**, with password *initialmd5*

You can change any of these as appropriate for your network installation. You can also override the defaults for any individual device or set of devices when you initially add the devices to the EPICenter inventory database, or by using the **Modify Devices and Device Groups** function at a later time.

Creating and Using Device Groups

EPICenter uses the concept of Device Groups to allow you to group devices with common features or functions. This allows you to work with multiple devices as a unit for a number of purposes within EPICenter.

For example, you might create Device Groups that represent devices by physical location, such as buildings, floors, or closets. You could create logical groupings such as device groups for your core devices, your edge devices, or all devices belonging to departments (engineering, sales, etc.). You could also create Device Groups for devices with common maintenance or management features, such as passwords or community strings in common.

A single device can belong to multiple device groups, so you can use Device Groups in many different ways. For example, you can scope alarms to specific device groups, so you can set up different levels of fault detection for different classes of devices. Functional device groups allow you to perform functions

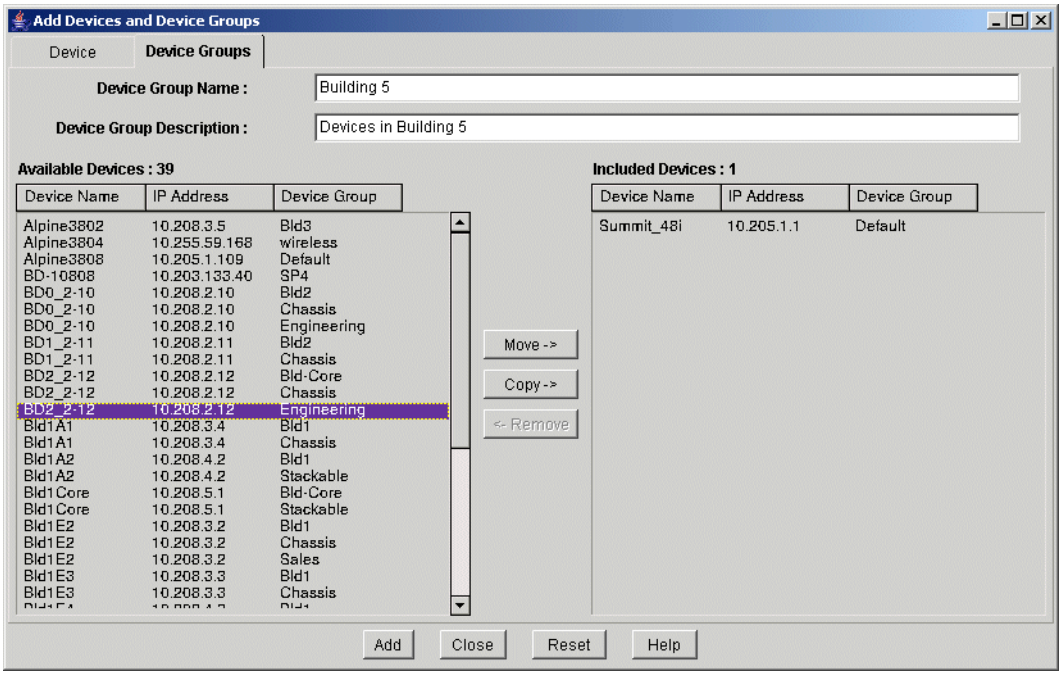
such as upgrading software versions or changing passwords on devices as a group, rather than one-by-one. Later chapters in this guide will provide examples of how device groups can be used for specific purposes in EPICenter.

Initially, EPICenter provides a single device group, named **Default**. This is where Discovery places the devices you add to the inventory, unless you specify a different device group. You can create additional device groups and place devices in those groups as you see fit.

To create a Device Group, click the **Add** button at the top of the page to bring up the **Add Devices and Device Groups** dialog, then click the **Device Groups** tab.

After providing a name and a description for your new group, you can specify the devices that should be included in the group. The Available Devices list shows you all the devices available to be placed in the new device group.

Figure 7: Adding a device group



As shown in Figure 7, there are several things to note about adding devices to a device group.

- If a device is already in multiple device groups, it is shown multiple times in the Available Devices list. (The highlighted switch, BD-2-12 is an example of this.)
- You can either **Move** or **Copy** a device to the new device group. **Move** removes the device from the old device group as it places the device in the new group. **Copy** leaves it in the old group as well as placing it in the new group.

  If you move the device, make sure you select the correct instance of the device in the Available Devices list, so it is removed from the correct device group.

Once a device group has been created, you can add or remove devices at any time using the **Modify Devices and Device Groups** function.

NOTE

Removing a device from all device groups does not remove the device from the database. The device is automatically placed back in the Default device group. if it is removed from all other device groups.

Managing Device Configurations and Firmware

EPICenter provides two features that can help you manage the configuration files and the firmware versions on your devices.

- The Configuration Manager provides an interface for uploading and saving backup configurations from your devices. You can upload configuration files from your devices on an "as needed" basis, or on a regular schedule. You can also save configuration files as "baseline" files for your devices, and then compare those baselines against newly uploaded configuration files to determine if changes have been made. The Configuration Manager also provides an interface you can use to download a saved configuration to a device.
- The Firmware Manager helps you manage the versions of firmware installed on your devices. EPICenter will check the Extreme Networks web site to find the most current versions of the device, slot and bootROM software, and will download it to the EPICenter server if you so choose. It can tell you if the software on your devices is the most current versions, and can also manage the process of the upgrading the images on your devices, through its Upgrade Wizard. Since there are multiple versions of software for different device and module types, and the software images and bootROM versions must also be compatible, the Firmware Manager can warn you if you attempt a download that may not be compatible with the device you have selected.

Once you have added your devices to the EPICenter Inventory Database, it is a good idea to save a set of baseline configuration files to use as a reference for identifying configuration changes to your devices. It is also a good idea to set up a regular schedule for uploading configuration files for archiving.

Periodically it is also a good idea to check for newer releases of the software and bootROM images for your Extreme devices. You can then download them to the EPICenter server, where they will be available for download to your devices when you decide to upgrade those devices.

Saving Baseline Configuration Files in the Configuration Manager

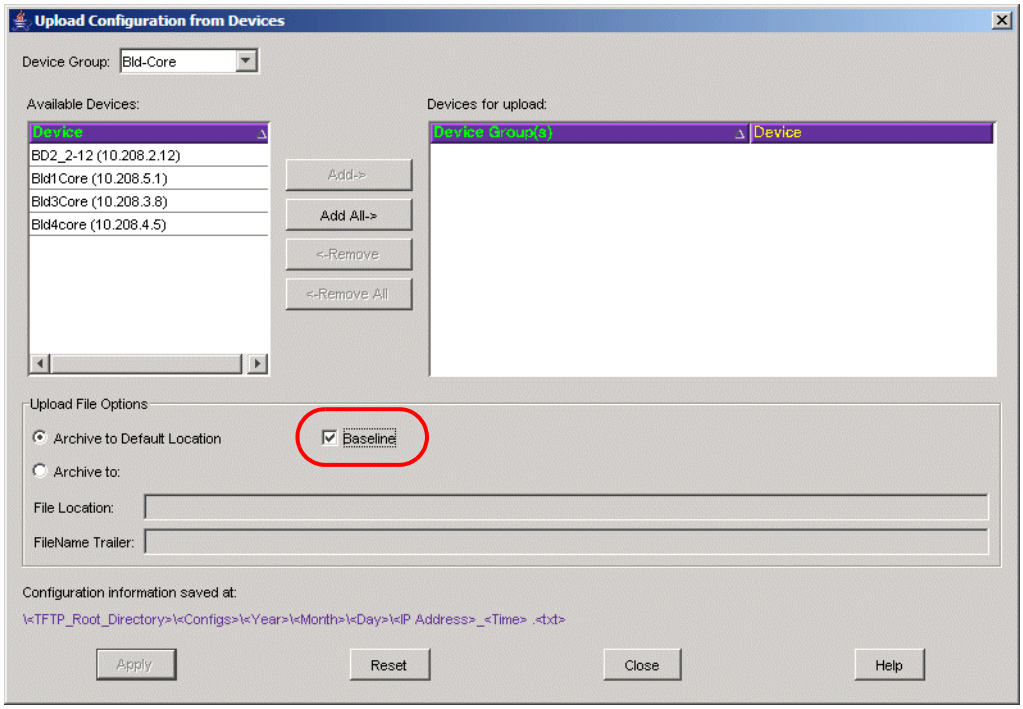
You can use the Configuration Manager to upload configuration files for backup purposes, or to create baseline configurations for your devices.

You can create baseline configurations in three ways:

- By uploading a configuration and designating it as a baseline configuration
- By scheduling a baseline configuration upload
- By selecting an existing saved configuration file to be used as a baseline configuration.

To upload a configuration as a baseline configuration file, you click **Upload** form the Config menu or from the toolbar to open the **Upload Configuration from Devices** window. Leave the Upload File Options set to **Archive to Default Location,** and also check the **Baseline** checkbox, as shown in Figure 8.

Figure 8: Uploading a Baseline Configuration File



This saves the configuration file as a baseline file in the `user/tftp/baselines` directory, named by ip address (e.g. `10_205_1_5.txt`).

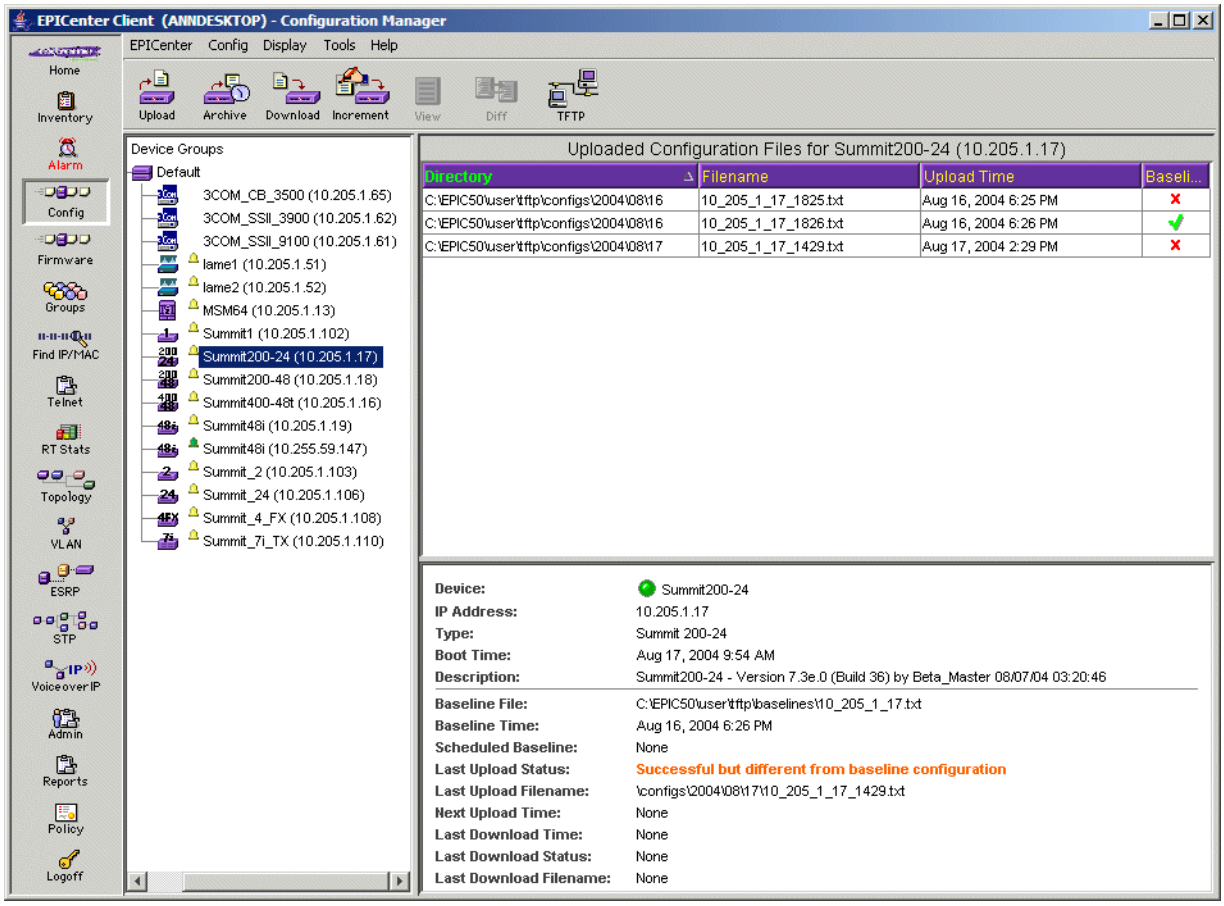
Note that you can also schedule the upload of baseline files. This feature is similar to scheduling archival uploads, except that a baseline upload cannot be scheduled on a repeating basis. However, this does let you schedule your baseline uploads to minimize impact on your network.

When a baseline file has been saved for a device, the Device display indicates which configuration file is the one that became the baseline file (as shown in Figure 9). Subsequent configuration uploads are compared to the baseline, and if changes were made that fact is noted.

Further, if you schedule regular archive configuration file uploads, EPICenter compares the newly-archived file against the baseline file to detect if there are difference, and creates a report that specifies exactly what those differences are, and also inspects the devices Syslog file to attempt to identify entries that could explain or be related to the configuration changes detected in the new archived configuration file.

See “Automatic Differences Detection” on page 95 for an example of report created when differences are detected.

Figure 9: Configuration file information for a device



Scheduling Configuration File Archiving

You can schedule regular archival configuration file uploads on a daily or weekly basis. You can also set a limit on how many configuration files per device will be saved (you can limit by time, or by the number of files). The archive feature can initiate uploads from multiple devices concurrently, thus speeding up the process of backing up the configurations from your devices.

To schedule uploads on a regular basis, click **Archive** or select the Archive command from the Config menu.

The Schedule Upload window has three tabs:

- From the **Device Schedule** tab you can select a set of devices you want to upload, in a similar manner to performing a regular upload, but you also specify a repeating schedule. You can schedule archive uploads to occur as follows:

  — Every day at a time you specify

  — Once a week on the day and at the time you specify

  You can create different schedules for different sets of devices, or for individual devices.

- From the **Global Schedule** tab you can set an archive schedule for all devices other than those that have individual or group schedules set. The Global Schedule lets you set an archive schedule for "everyone else."

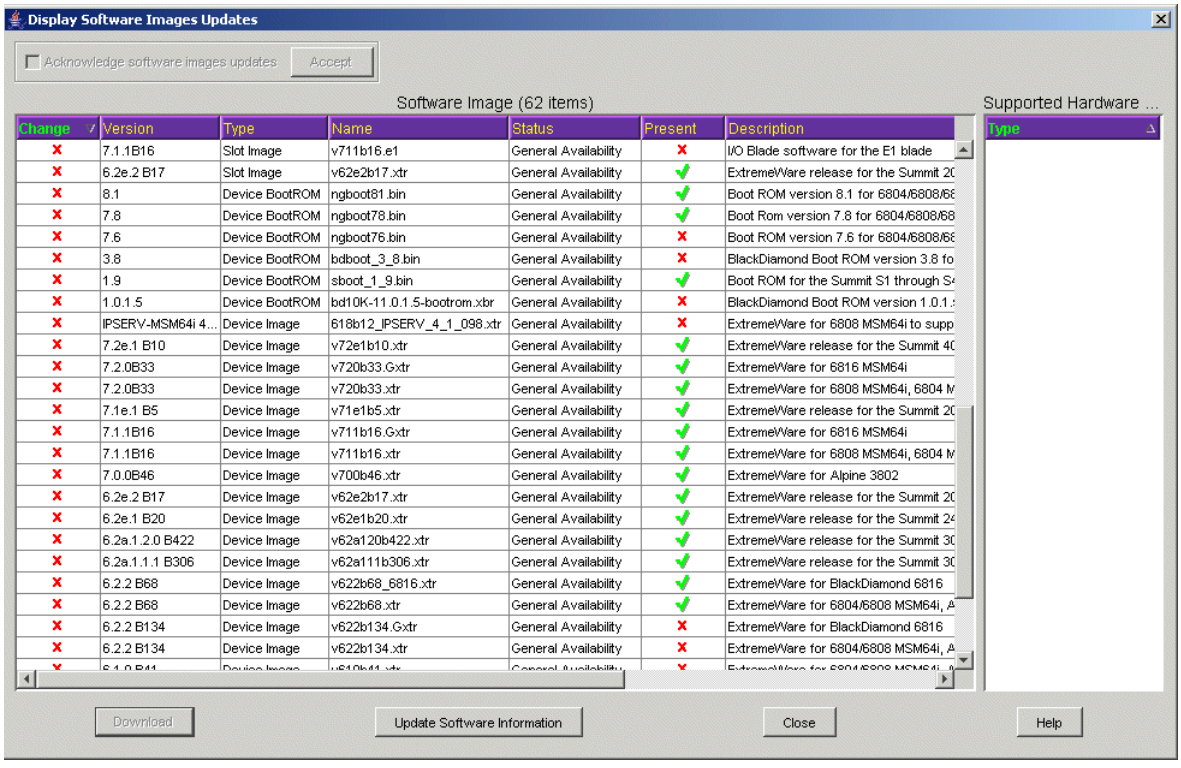
- From the **Archive Limit** tab you can limit the number of configuration files that will accumulate over time. The limits operate per device. You can limit the number of saved configuration files either by number or by time. For example, a limit of 10 copies means that after 10 files have been saved for a device, when the 11th file is uploaded, the oldest saved file is deleted. A limit of 7 days means that saved configuration files more than 7 days old are deleted. This creates an upper limit on the amount of space that will be consumed by saved configuration files.

Checking for Software Updates

Another area where EPICenter can provide a valuable service is in keeping track of the software versions on your network devices. The Firmware Manager not only reports on the software and bootROM versions running in your devices, but also can continually check the Extreme Networks web site to determine if new versions have been released.

When you install EPICenter you can enable the **Automatic Information Update** feature. This feature will connect to the Extreme Networks web site when the EPICenter server starts up, and then once every 24 hours, to check for new software updates. If it does find updates, it displays a message when you log into the EPICenter server from an EPICenter client, giving you the option of opening the **Display Software Images Updates** page. The Display Software Images Updates page shows all the software and bootROM versions available for both devices and modules, along with an indication of whether these versions have been updated since the last time you checked for (and accepted) update information.

Figure 10: The Display Software Images Updates window


Display Software Images Updates
Acknowledge software images updates
Accept
Software Image (62 items)
Supported Hardware ...
Change
Version
Type
Name
Status
Present
Description
Type
7.1.1B16 Slot Image v711b16.e1 General Availability I/O Blade software for the E1 blade
6.2e.2 B17 Slot Image v62e2b17.xtr General Availability ExtremeWare release for the Summit 2
8.1 Device BootROM ngboot81.bin General Availability Boot ROM version 8.1 for 6804/6808/6
7.8 Device BootROM ngboot78.bin General Availability Boot Rom version 7.8 for 6804/6808/68
7.6 Device BootROM ngboot76.bin General Availability Boot ROM version 7.6 for 6804/6808/6
3.8 Device BootROM bdboot_3_8.bin General Availability BlackDiamond Boot ROM version 3.8 fo
1.9 Device BootROM sboot_1_9.bin General Availability Boot ROM for the Summit S1 through S
1.0.1.5 Device BootROM bd10K-11.0.1.5-bootrom.xbr General Availability BlackDiamond Boot ROM version 1.0.1.
IPSERV-MSM64i 4... Device Image 618b12_IPSERV_4_1_098.xtr General Availability ExtremeWare for 6808 MSM64i to supp
7.2e.1 B10 Device Image v72e1b10.xtr General Availability ExtremeWare release for the Summit 4
7.2.0B33 Device Image v720b33.Gxtr General Availability ExtremeWare for 6816 MSM64i
7.2.0B33 Device Image v720b33.xtr General Availability ExtremeWare for 6808 MSM64i, 6804 M
7.1e.1 B5 Device Image v71e1b5.xtr General Availability ExtremeWare release for the Summit 2
7.1.1B16 Device Image v711b16.Gxtr General Availability ExtremeWare for 6816 MSM64i
7.1.1B16 Device Image v711b16.xtr General Availability ExtremeWare for 6808 MSM64i, 6804 M
7.0.0B46 Device Image v700b46.xtr General Availability ExtremeWare for Alpine 3802
6.2e.2 B17 Device Image v62e2b17.xtr General Availability ExtremeWare release for the Summit 2
6.2e.1 B20 Device Image v62e1b20.xtr General Availability ExtremeWare release for the Summit 2
6.2a.1.2.0 B422 Device Image v62a120b422.xtr General Availability ExtremeWare release for the Summit 3
6.2a.1.1.1 B306 Device Image v62a111b306.xtr General Availability ExtremeWare release for the Summit 3
6.2.2 B68 Device Image v622b68_6816.xtr General Availability ExtremeWare for BlackDiamond 6816
6.2.2 B68 Device Image v622b68.xtr General Availability ExtremeWare for 6804/6808 MSM64i, A
6.2.2 B134 Device Image v622b134.Gxtr General Availability ExtremeWare for BlackDiamond 6816
6.2.2 B134 Device Image v622b134.xtr General Availability ExtremeWare for 6804/6808 MSM64i, A
Download
Update Software Information
Close
Help

From the Display Software Images Updates window you can select software images to download to the EPICenter server, where they will then be available for download onto your devices. In Figure 10, the images with green checks in the **Present** column have been uploaded to the EPICenter server. The red

Xs in the **Change** column indicates that the versions on the Extreme Networks web site have changed since the last time this display was Accepted. The Accept button at the top left corner, along with the checkbox, are used to acknowledge the update information. This lets EPICenter know what version information you have received, so that it can tell when versions on the web site have changed.

Note that the first time you display the software images information, all images will be noted as being changed, as none of the information has yet been accepted.

The Firmware Manager does not automatically download software to a device. However, by having the images available on the EPICenter server, you can download them to your devices on whatever schedule you want. You can also perform downloads to groups of compatible devices in a single operation. EPICenter can initiate multiple downloads concurrently, which increases the efficiency and reduces the time required when you need to upgrade multiple devices.

Using the EPICenter Alarm System

The EPICenter Alarm System provides fault detection and alarm handling for the network devices monitored by EPICenter. This includes Extreme Networks devices as well as some third-party devices—those that EPICenter can include in its Inventory database.

The Alarm System provides a set of predefined, enabled alarms that will immediately report conditions such as authentication or login failures, device problems such as power supply or fan failures, reachability problems, or device reboots. You can also define your own alarms that will report errors under conditions you specify, such as repeated occurrences or exceeding threshold values. You can specify the actions that should be taken when an alarm occurs, and you can enable and disable individual alarms.

The Alarm button in the Navigation Toolbar also acts as an alarm indicator—it appears in red when alarms have occurred that have not been acknowledged.

Fault detection is based on SNMP traps, syslog messages, and some limited polling. The Alarm System supports SNMP MIB-2, the Extreme Networks private MIB, RMON traps, and selected traps from other MIBs. When an alarm occurs you can specify actions such as sending e-mail, running a program, running a script, sending a page or sounding an audible alert. You can also forward the trap to another trap receiver.

Predefined Alarms

For convenience, the EPICenter Alarm System provides a number of predefined alarms. These alarms are enabled by default and are active as soon as the EPICenter server starts up. These include the following alarms:

- Authentication failure (SNMP MIB-2 trap)
- Config Upload Failed (EPICenter event, indicates failure in an upload initiated by EPICenter)
- Device reboot (EPICenter event)
- Device Warning from EPICenter (EPICenter event)
- ESRP State Changed (Extreme proprietary trap)
- Fan failure (EPICenter event)
- Health Check Failed (Extreme proprietary trap)

- Invalid login (Extreme proprietary trap)
- Overheat (EPICenter event)
- Power Supply Failed (EPICenter event)
- Rogue Access Point Found (EPICenter event)
- Redundant Power Supply (RPS) alarm condition (Extreme proprietary trap)
- SNMP unreachable (EPICenter event)

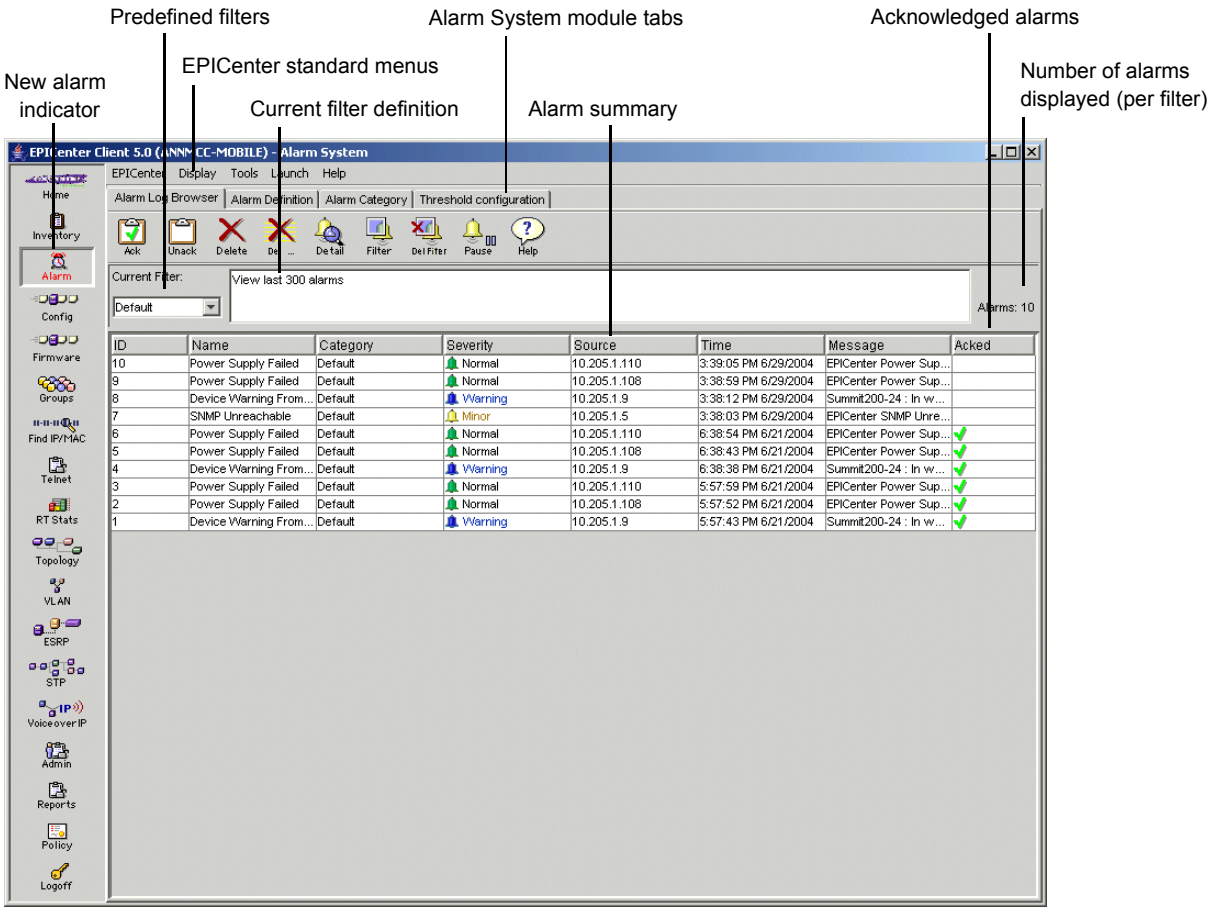
NOTE

When Extreme Networks devices are added to the EPICenter Inventory database, they are automatically configured to send traps to the EPICenter server (unless you are running in non-intrusive Mode). To receive traps from non-Extreme Networks devices, you must manually configure those devices to send traps to the EPICenter server. See Appendix B in the EPICenter Reference Guide for information on registering EPICenter as a trap receiver on non-Extreme devices.

The Alarm Log Browser

You use the Alarm Log Browser to view a summary of the alarms that have occurred among the devices you are managing. An alarm can be generated due to an SNMP or RMON trap, a syslog message, or based on the results of a poll. By default, all the predefined alarms are enabled; therefore, you may see alarm log entries the first time you display the Alarm Browser, even if you have not defined any alarms of your own.

Figure 11: The Alarm Log Browser page



Filtering the Alarm Log Display

You can filter the list of alarms to view only a subset of alarms that are of particular interest—only alarms from a specific device, or a specific type of alarm, for example. The default filter displays the last 300 alarms from the EPICenter database (unless you had a device selected in the previous applet when you opened the Alarm Browser, in which case the display will be filtered for alarms on the selected device). There are three other predefined display filters based on time: “7 days ago,” Last 24 hours,” and “Yesterday.” You can also create display filters to view any subset of alarms that you wish.

If you have selected a device in another applet when you open the Alarm Browser, or if you invoke the Alarm Browser from the Devices sub-menu of a right-click menu, the default filter is set for the IP address of device that was selected. You can save that filter for later re-used, if you wish.

You can also create your own filters based on a variety or combination of criteria such as Source IP, Severity, Alarm Name, LogID, and a number of others. Your filter can combine multiple criteria.

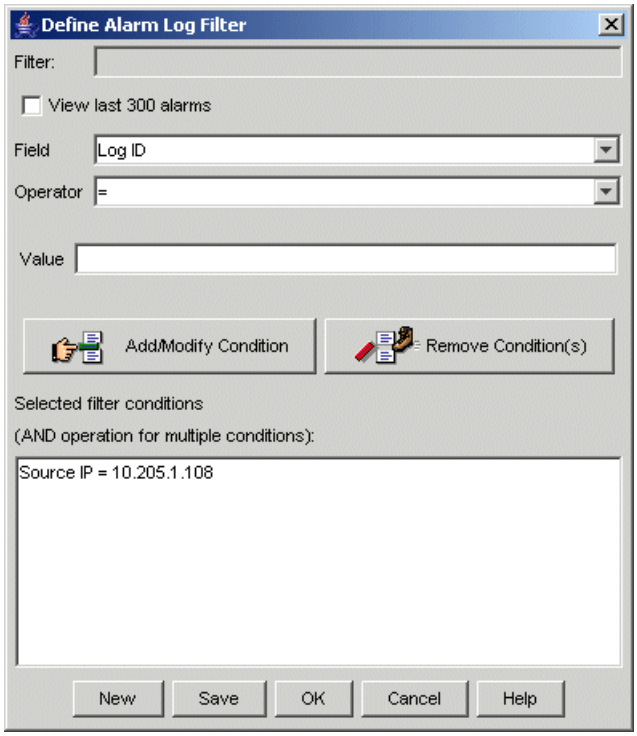
Example: Filtering the Alarm Log Display for a Device IP Address

Filter the list of alarms to view only alarms from the device at IP address 10.205.1.108

1 Click the **Filter** button at the top of the Alarm Summary window.

The Define Alarm Log Filter window opens.

Figure 12: The Alarm Log filter definition window



2 Uncheck the **View last 300 alarms** checkbox.

3 From the drop-down menu in the **Field** field, select **Source IP**.

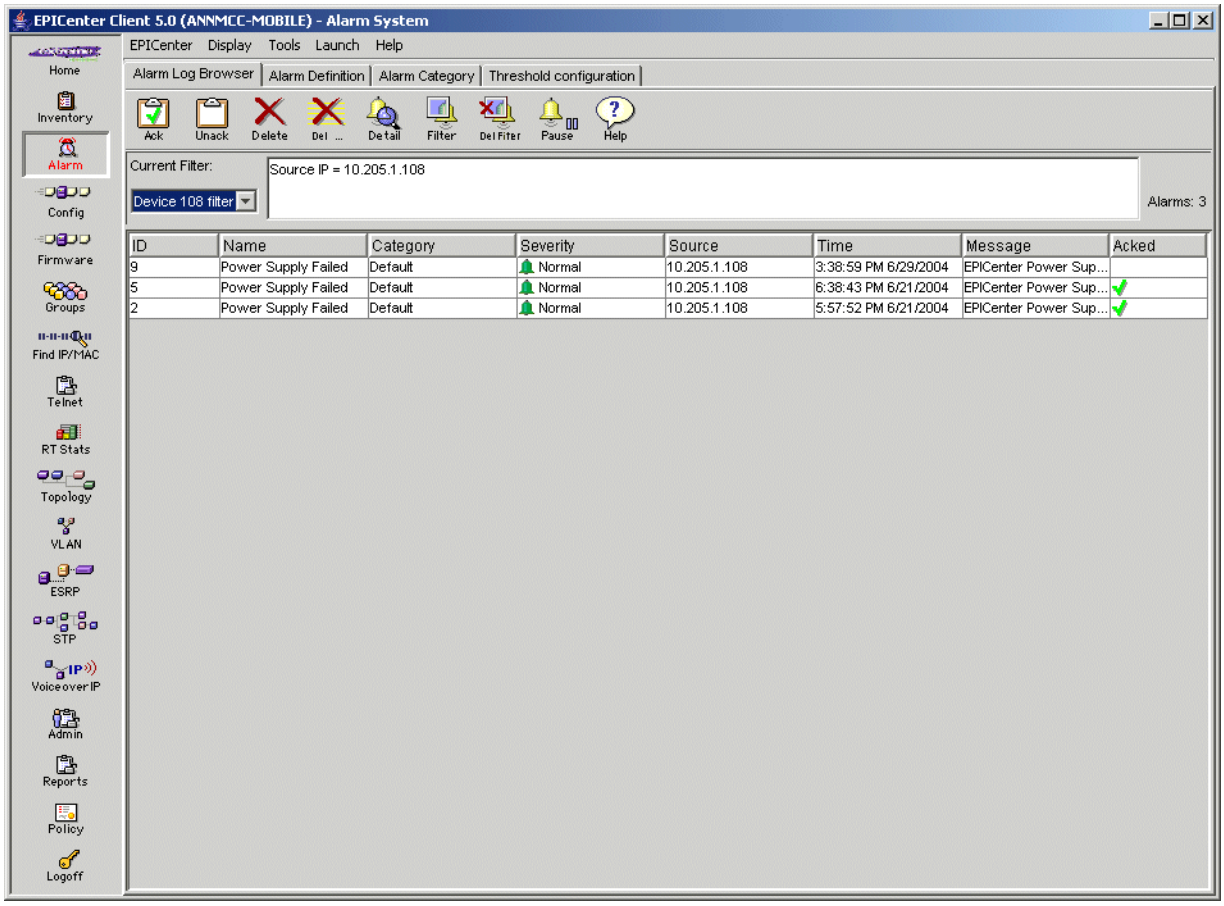
4 Enter the IP address into **Value** field.

5 Click **Add/Modify Condition**. This adds the condition "Source IP = 10.205.1.108" to the list of conditions that EPICenter will use to filter the alarm list.

6 Click **OK** to display the alarms that match this filter.

The Alarm Summary is refreshed to show only the alarms that match your filter.

Figure 13: The filtered alarm summary list



7 If you want to save this filter for future use, click the **Filter** button again. The Define Alarm Log Filter window again opens, displaying the filter definition you just created.

8 Click **Save** and another small window opens where you can enter a name for this filter. Type a name and click **OK** to save this filter.

Once you have saved your filter, you will be able to select it from the drop-down filter list in the main Alarm Browser window.

You can create a filter that uses several conditions, but you cannot filter using multiple specifications of the same condition. Multiple conditions are combined using a logical AND function—all conditions must be matched for an alarm entry to be included in the filter results. For example, you can filter for "Source IP = 10.205.1.108" and "Severity = Critical." This will display all alarms for the device with severity levels of critical.

However, in order to find and view alarms for IP addresses 10.205.1.108 and 10.205.1.110, you must use the **Between** operator to test for all Source IP addresses between these two IP addresses. You cannot create a filter that includes separate condition specifications for Source IP = 10.205.1.108 and Source IP = 10.205.1.110.

Creating or Modifying an Alarm Definition

Although EPICenter provides a number of predefined alarms, you may find that you need to modify those alarm definitions, or even create your own alarms to alert you to specific conditions. For example, you may decide to modify the predefined SNMP Unreachable alarm to send an email to the network administrator when a device becomes unreachable (the predefined alarms by default do not take any actions other than to create an entry in the alarm log). Or, you may decide to create a new alarm that alerts you when CPU utilization on a device exceeds a threshold (utilization rises above 80%, for example).

An alarm definition has three parts:

- The *basic alarm properties*, which include the event-related parameters of the alarm: its name, severity, the event that will trigger it, and so on.
- The *alarm actions*, which are functions that the alarm system executes when an alarm occurs, in addition to logging the alarm event. Alarm actions can include sending e-mail, sounding an audible alert, running a program or executing a script.
- The *alarm scope*, which defines the devices that can trigger an alarm.

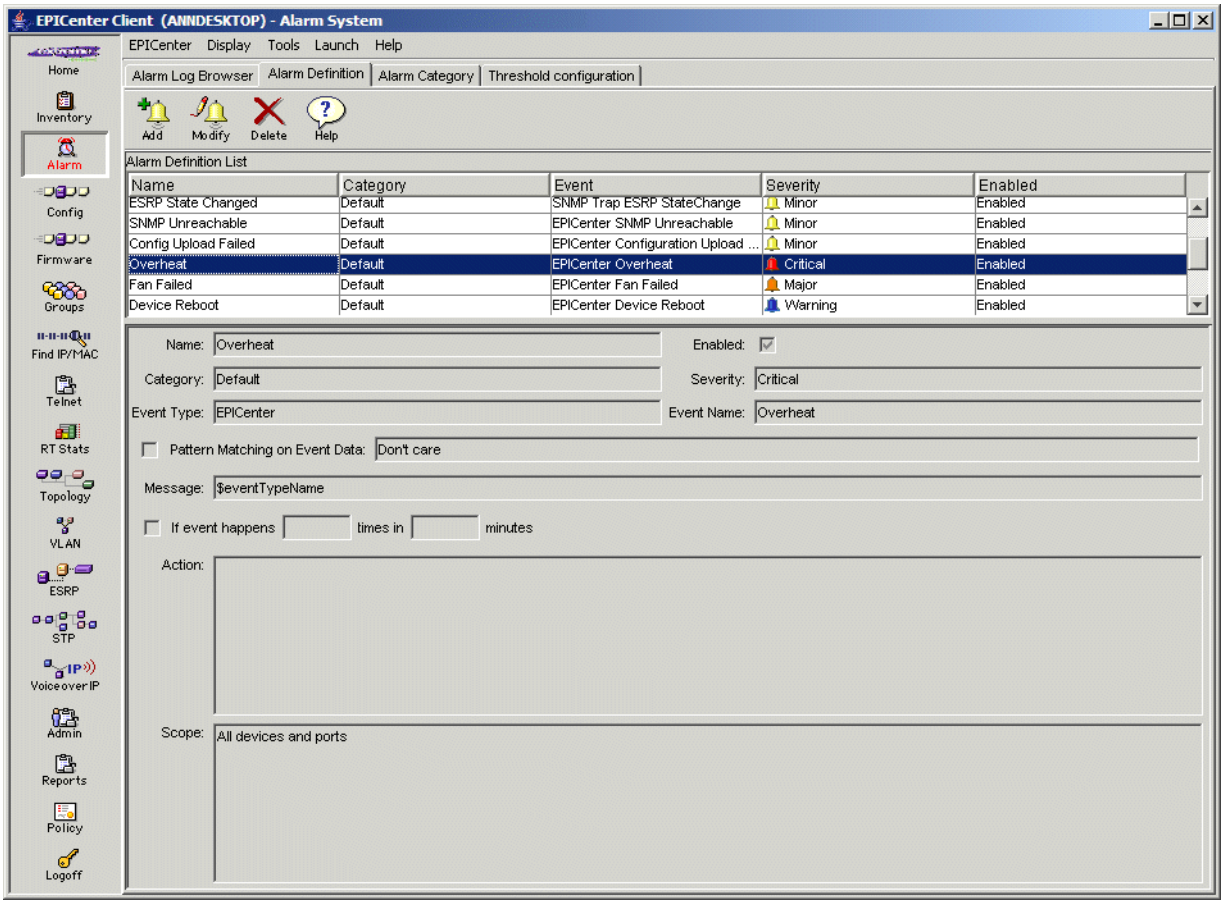
The following examples show how you configure these three aspects to define an alarm.

Example 1: Modifying a Predefined Alarm to Send a Text Page

Modify the Overheat alarm so that it will page the network administrator at “4083236789@paging.com” if an overheat condition is detected.

1 Click the **Alarm Definition** tab at the top of the window. This displays the Alarm Definition List.

Figure 14: The Alarm Definition List with the Overheat alarm selected

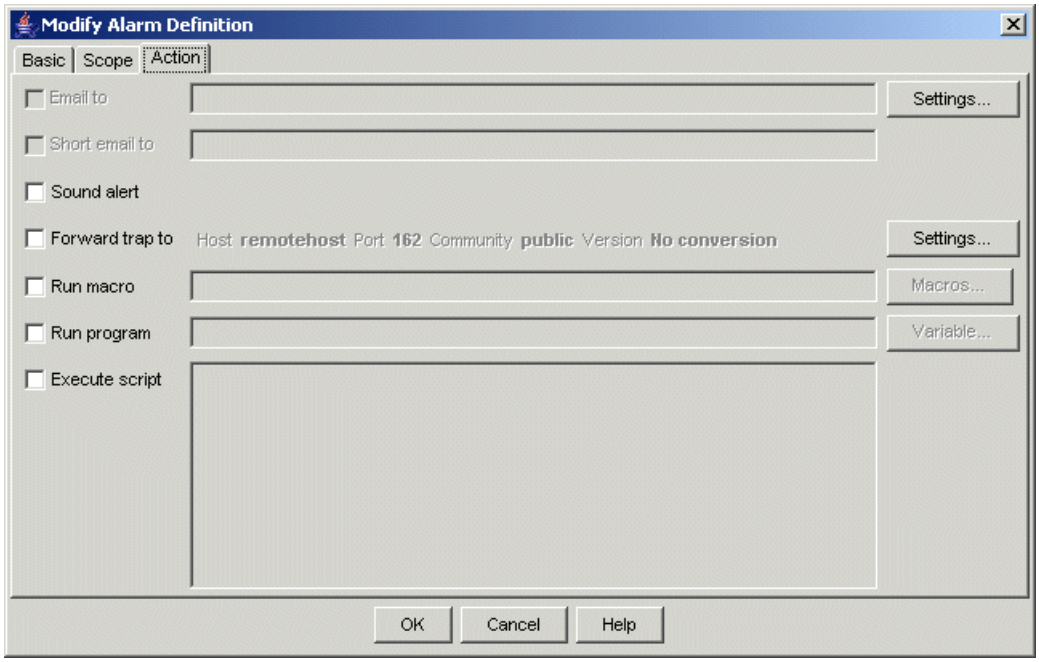


2 Scroll down in the list and select the Overheat alarm definition. The basic properties for this alarm definition are displayed in the lower part of the page when you do this, as shown in Figure 14.

3 Click the **Modify** button. A Modify Alarm Definition dialog appears, with the **Basic** properties tab displayed.

4 Click the **Action** tab to display the alarm actions available.

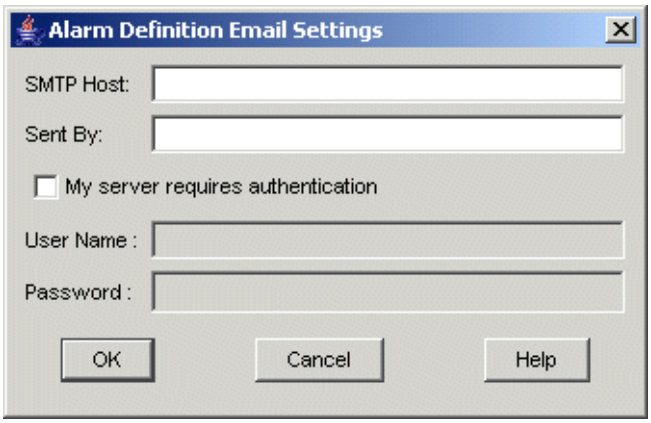
Figure 15: The Modify Alarm Definition window with the Action Tab displayed



For this alarm, you want to use an email action. However, before you can specify an email action, you must configure EPICenter with settings for the SMTP server it should use. If this has not yet been done, the two email checkboxes are not selectable, as shown in Figure 15.

5 To configure EPICenter's email settings, click the **Settings...** button to the right of the **Email to** field. This opens the Alarm Definition Email Settings dialog.

Figure 16: The Email Settings dialog



a Enter the host name or IP address of the SMTP server EPICenter should use.

b Enter the sender ID for all email sent by EPICenter.

c If the outgoing mail server requires authentication (an ID and password) check the box and enter a valid ID and password into the fields provided.

If you don't know whether your server requires authentication, you can go ahead and enter the authentication information—it will be ignored if it is not actually needed.

d Click **OK** to save these settings.

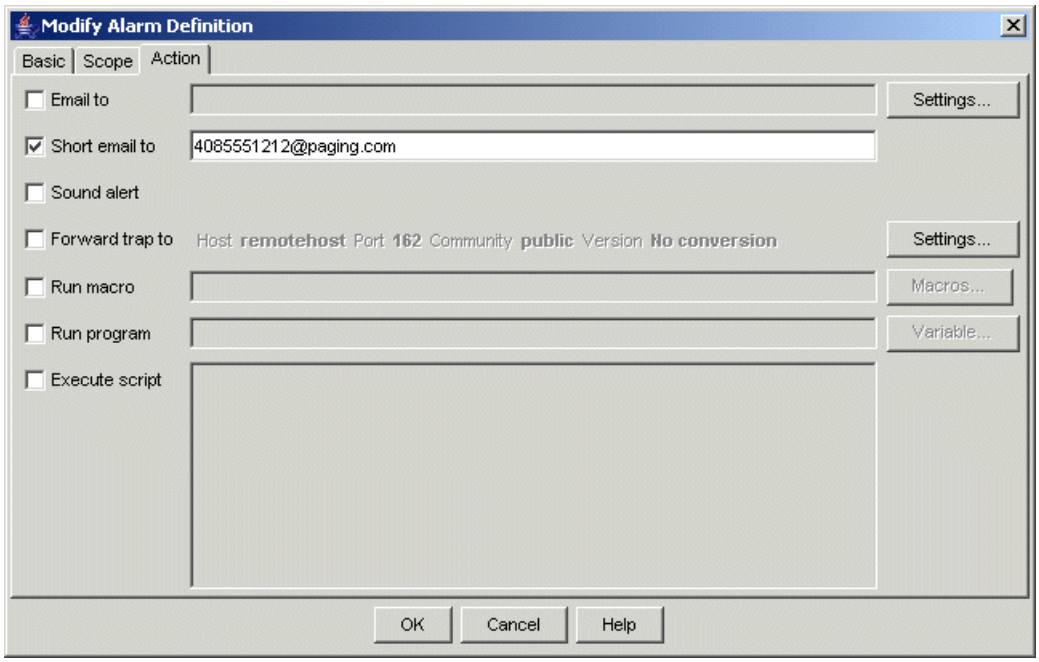
NOTE

If your e-mail server is not reachable when an alarm action attempts to send an email, the alarm server may stall waiting for the email server to respond.

6 To configure EPICenter to send a text message as an alarm action, click the **Short email to:** check box to turn on the check.

7 Type **`4085551212@paging.com`** as the email address in the text field next to the checkbox, as shown in Figure 17.

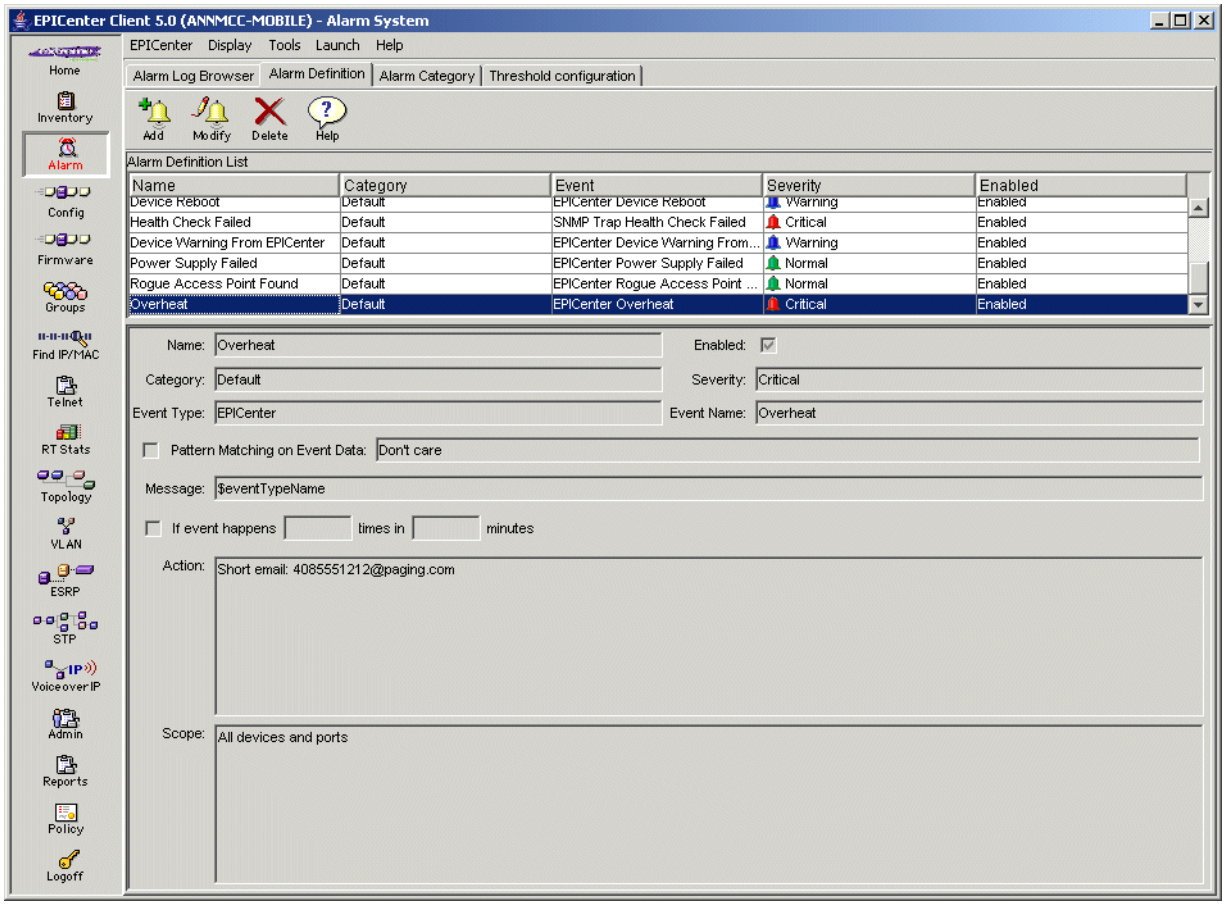
Figure 17: A short email action defined for text paging



8 Click **OK** to finish the alarm definition.

The modified alarm definition is displayed in the Alarm Definition List as shown in Figure 18.

Figure 18: The modified Overheat alarm



Example 2: Define a New Alarm to Forward a Trap

Define a new alarm that forwards a trap to a remote host if port 10 on device "Summit_24" goes down.

1 Click the **Alarm Definition** tab at the top of the window, then click **Add** to open the New Alarm Definition dialog with the **Basic** tab displayed.

   a Type a name for the alarm (for example, **WAN Link Down**) in the **Name** field.

   b Make sure the **Enabled** checkbox is checked.

   c Select a severity level in the **Severity** field

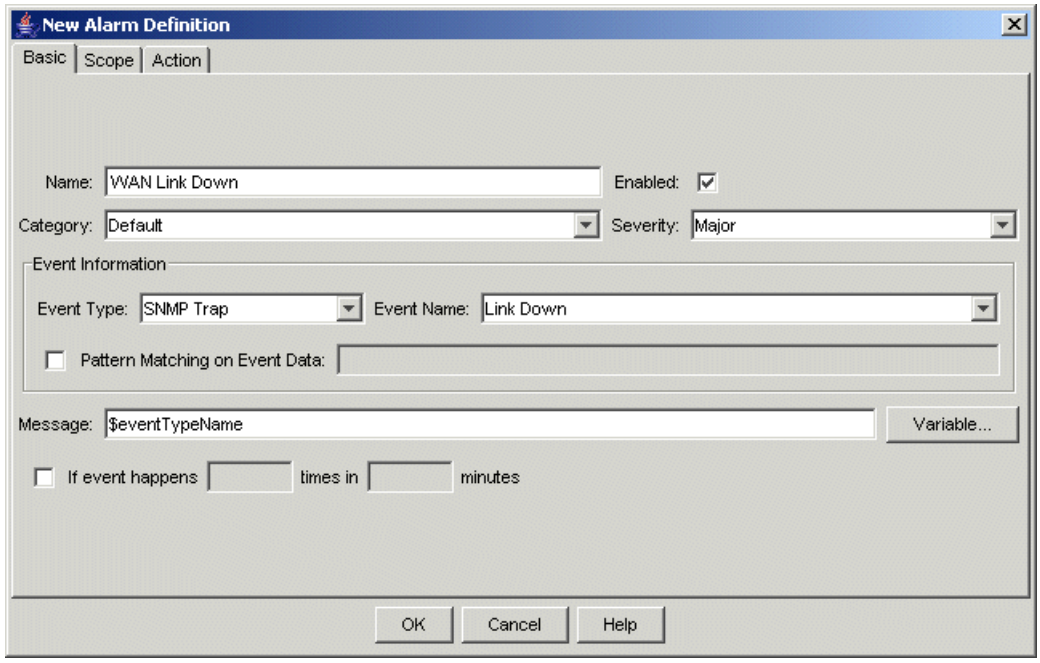
   d Select a category (e.g. "Default") in the **Category** field.

   e Select "SNMP Trap" in the **Event Type** field.

   f Select "Link Down" in the **Event Name** field.

   The information in the **Basic** tab should look as shown in Figure 19.

Figure 19: The Basic tab of the New Alarm Definition window



2 Click the **Scope** tab, and do the following:

a Make sure the **All devices and ports** checkbox is not checked.

b Select "Port" in the **Source Type** field.

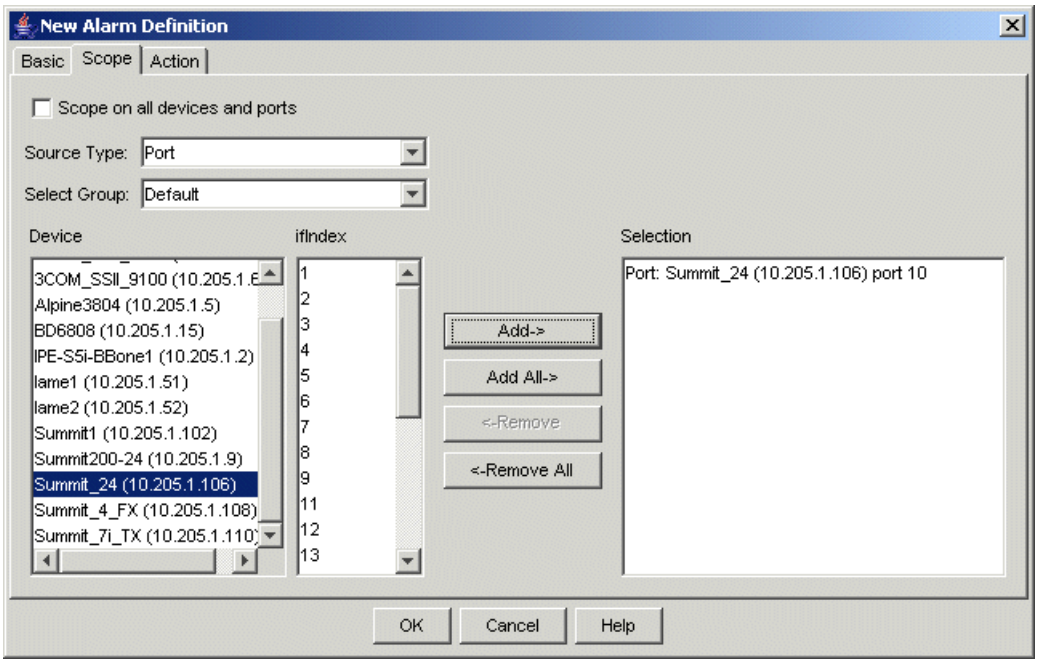
c Select the device ("Summit_24") from the **Device** list.

d Select the port ("10") from the **ifIndex** list.

e Click the **Add** button to add Summit_24 port 10 to the **Selection** list.

The information in the **Scope** tab should look as shown in Figure 20.

Figure 20: The Scope tab of the New Alarm Definition window



NOTE

For convenience in scoping alarms, you might want to consider creating special-purpose device groups or port groups, and use those in your alarm scope. The benefit is that you can change the scope of the alarm simply by changing the membership of the relevant group. You will not need to modify our alarms every time you add, move or change elements in your network —adding or removing ports or devices from the relevant devices groups will be sufficient.

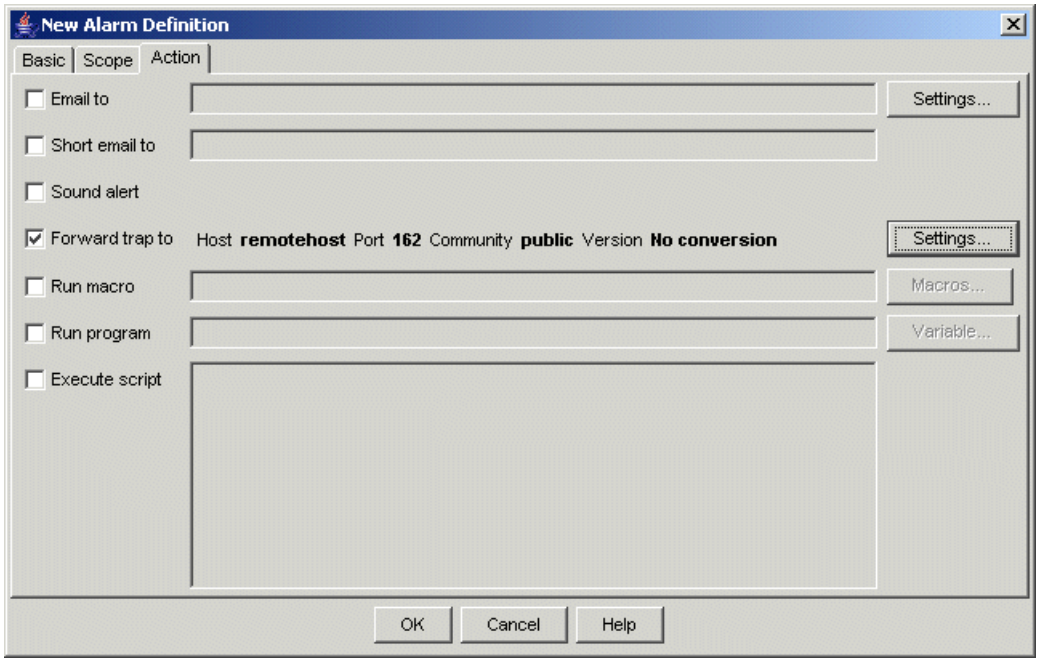
3 Click the **Action** tab, and do the following:

a Click the **Forward trap to:** check box to turn on the check.

When the checkbox is checked, a line showing the trap receiver configuration is displayed. The trap receiver is defined by a host name, port, community string, and whether the trap should be converted to SNMPv1 or SNMPv2c.

The information in the **Action** tab should look as shown in Figure 21.

Figure 21: The Action tab of the New Alarm Definition window



b If you need to change the trap receiver configuration, click the **Settings...** button to the right of the **Forward trap to:** line. This opens a configuration dialog where you can change the trap receiver configuration.

4 Click **OK** to finish the alarm definition.

Threshold Configuration for RMON and CPU Utilization Alarms

Through EPICenter you can define threshold conditions that, when exceeded, will cause a trap event to occur. You can define thresholds for CPU utilization and for a wide range of RMON variables. Several RMON conditions, specifically for port utilization, temperature, and STP topology changes, have been partially predefined to make the rule definition process easier. There are other SNMP traps supported by the EPICenter Alarm System that are not included in the EPICenter threshold configuration function, where the threshold conditions can be configured directly on the switch.

With threshold events, traps are generated based on comparing the value of the relevant sample variable with the threshold value. You create rules that specify the threshold values, define the target devices on which the event rules should be configured, and in turn use those rules in EPICenter alarm definitions that specify the actions to be take when a sample value crosses the threshold specified in the rule.

When you create a rule, you can specify both a Rising Threshold and a Falling Threshold, if appropriate.

- A Rising Threshold means that a trap is generated when the value of the RMON variable increases past the threshold value. If only a Rising threshold is specified, then no trap is generated if the value decreases past the threshold.
- A Falling Threshold means that a trap is generated when the value of the RMON variable decreases past the threshold value. If only a Falling threshold is specified, then no trap is generated if the value increases past the threshold.

If you want a trap event to occur for both Rising and Falling threshold conditions, you can specify both thresholds.

There are other SNMP traps supported by the EPICenter Alarm System, but not included in the threshold configuration function, that may require conditions to be set on the switch to define when a trap should occur. See Appendix B, "Configuring Devices for Use with EPICenter" in the *EPICenter Reference Guide* for additional information.

NOTE

Creating the rules that control trap (event) generation is only the first of the two steps required to create EPICenter alarms for these events. Even though you have set up these rules, the trap events generated as a result will be ignored by the Alarm System until you define alarms that take actions on those events. See "Creating or Modifying an Alarm Definition" on page 46 for more information.

There are two parts to an event rule; the rule configuration itself, and the association of the rule to its target devices.

NOTE

CPU Utilization is only supported on switches running ExtremeWare 6.2 or later. STP Topology change traps are only supported on switches running ExtremeWare 6.2.2 or later.

A new RMON rule is added as a new "folder" in the Configuration Tree, and each target device for the rule appears as a separate component under that rule. The rule name will also appear in the Event Name list.

For CPU Utilization rules, each target device for a CPU utilization rule appears as a separate component under the CPU Utilization "folder" in the Configurations tree.

- **Startup Alarm:** The condition that should be met to cause the initial occurrence of this event. Select from the following:
  - **Rising**: an event will be generated the first time the sample value becomes greater than or equal to the Rising Threshold value. No events will be generated related to the Falling threshold until after this has occurred.
  - **Falling**: an event will be generated the first time the sample value becomes less than or equal to the Falling Threshold value. No events will be generated related to the Rising threshold until after this has occurred.
  - **RisingOrFalling**: an event will be generated the first time the sample value becomes either greater than or equal to the Rising Threshold value, or less than or equal to the Falling Threshold value.

How RMON Events are Generated

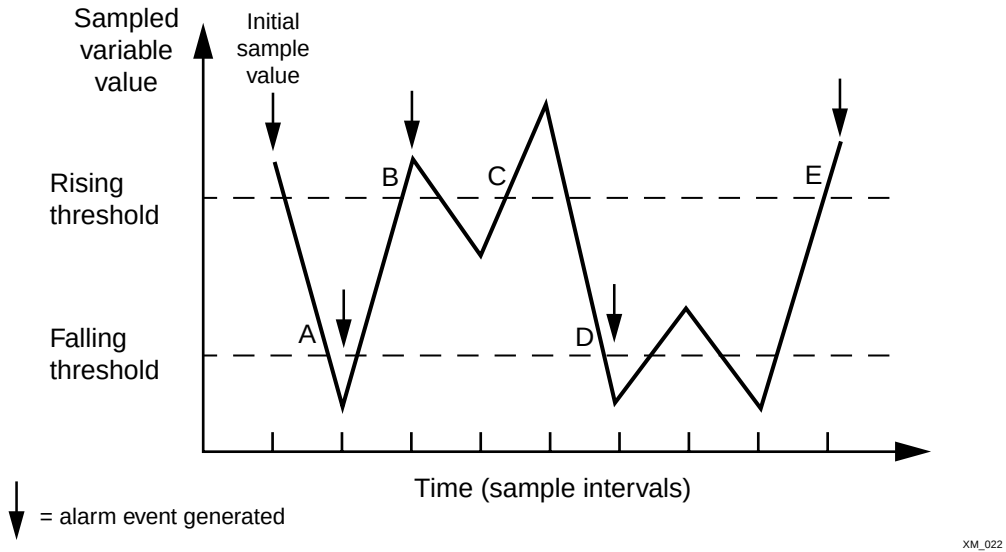
When you configure an RMON threshold condition, you must specify not only the value of the threshold, but also the startup alarm condition. The initial occurrence of an RMON alarm is determined by the Startup Alarm condition specified when the alarm is defined.

It is important to understand that, except for the initial occurrence of the alarm, an RMON alarm event will be generated only the when the sample value of the variable crosses one of the thresholds for the first time after having crossed the other threshold.

The following diagram, shown in Figure 22, shows how alarms are generated for an RMON rule using Delta values, where the startup alarm condition is set to “Rising” or “RisingOrFalling.”

RMON Alarm Event Generation

Figure 22: RMON Alarm event generation



Because the initial sample value of the variable is greater than the value of the Rising threshold, an RMON rising threshold trap is generated. A second trap occurs at the next sample interval (point A) because the sample variable value is now less than the Falling Threshold. At point B the value again passes the Rising Threshold, and another trap event is generated. However, no trap occurs at point C, even though the value of the variable again becomes greater than the Rising Threshold, because the value has not yet become less than the Falling threshold. Another Rising threshold trap event cannot occur until after a Falling threshold alarm has occurred, as happens at point D.

Note that in order to have any of these trap events cause an alarm in the EPICenter Alarm System, you need to define an alarm that responds to a RMON Rising Threshold or RMON Falling Threshold event.

- If you define an alarm based on the RMON Rising Threshold event, then EPICenter alarms will occur at the initial sample, and at points B and E. Because the alarm is defined to respond to RMON Rising Threshold events, the falling threshold trap events that occur at points A and D do not trigger an EPICenter alarm.
- If you also define an alarm based on an RMON Falling Threshold event, then EPICenter alarms would also be generated at points A and D.

Example 3: Create an RMON Rule to Detect Excessive Port Utilization

Example: Create an RMON rule that will cause an RMON Rising Trap when port utilization on a set of critical ports, members of the port group “CriticalPorts,” exceeds 15%.

1 Bring up the **New Configuration** dialog. On the **Configuration** page, do the following:

a Type a name for the rule in the **Name** field (for example, “WAN Link 15%”).

If you have already created an alarm definition that will use this rule, make sure the name matches the name you entered in the alarm definition.

b Click the **Look up...** button to display the **Select MIB Variable** dialog.

c Expand the Extreme folder, select the `extremeRtStatsUtilization` variable, and click OK to enter it into the **MIB Variable** field.

d Type "1500" in the **Rising Threshold** field. Note that for this variable the value must be in hundredths of a percent.

e Type a smaller value, for example "1450" in the **Falling Threshold** field.

f Leave the **Sample Type** as "Absolute" and the **Sample Interval** at the default value (15).

g Select **Rising** for the **Startup Alarm** field.

2 Click the **Target** tab and do the following:

a Select Port Group as the **Source Type**

b Select "CriticalPorts" from the **Port Groups** list

c Click **Add** to add the Port Group to the **Selection** list

3 Click the **Apply** button to configure the rule on the device ports that are members of the CriticalPorts port group.

A message window will appear with the device configuration results.

4 Verify that no switch configuration errors have been reported, and click **OK** to dismiss the window.

5 Click **Close** to dismiss the **New Configuration** dialog.

Configuring a CPU Utilization Rule

NOTE

CPU Utilization is only supported on switches running ExtremeWare 6.2 or later.

If you select CPU Utilization, only the Rising Threshold field allows input. The other fields and buttons in this window are predefined.

- **Rising Threshold—** A threshold value, in percent, that will trigger an event when the CPU utilization rises past this value. This value is also used to compute a falling threshold, which is defined as 80% of the rising threshold.

The other parameters that you can set when you configure an RMON event, are predefined in the Extreme switch agent for a CPU Utilization event. These are:

- **MIB Variable**: The MIB variable is predefined to be `extremeCpuUtilRisingThreshold.0`.
- **Falling Threshold**: This is predefined as 80% of the rising threshold
- **Sample Interval:** The sample interval for a CPU Utilization alarm is also predefined, and is set to 3 seconds
- **Sample Type**: The sample value (a percentage) is always an absolute value
- **Startup Alarm**: The Startup condition is predefined to be **Rising**

NOTE

To define an alarm for a CPU Utilization threshold event, select SNMP Trap as the Event Type, then select CPU Utilization Rising Threshold or CPU Utilization Falling Threshold as the Event Name.

If you define an alarm for a CPU Utilization Rising Threshold event, an alarm will be generated each time the sample value meets the following conditions:

— When the sample value becomes greater than or equal to the Rising Threshold for the first time (including the initial sample) after the alarm is enabled.

— The first time the sample value becomes greater than or equal to the Rising Threshold, *after having become less than or equal to the Falling Threshold* (80% of the Rising threshold).

If you define an alarm for CPU Utilization Falling Threshold events, an event will be generated each time the sample value meets the following conditions:

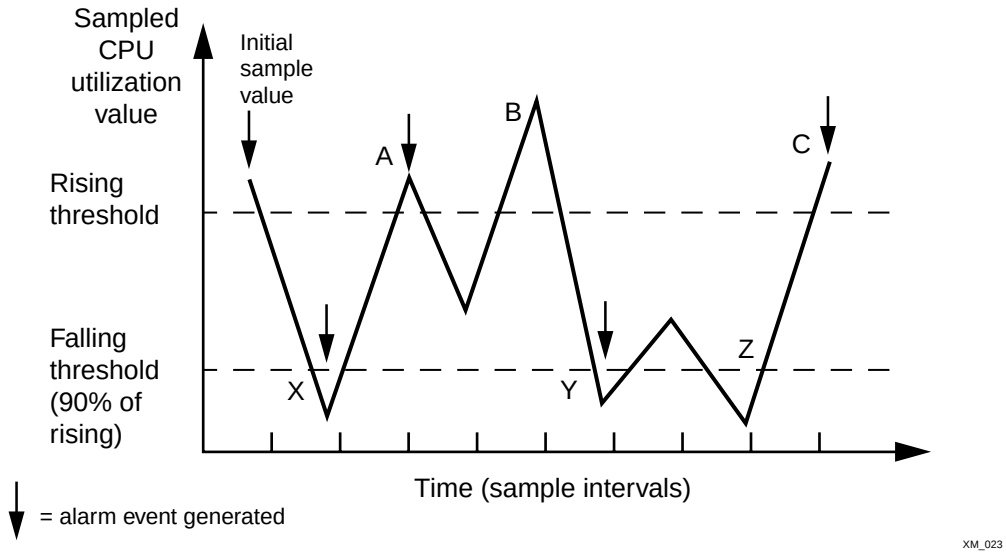
— The first time the sample value becomes less than or equal to 80% of the Rising Threshold, *after having become greater than or equal to the Rising Threshold*.

It is important to understand that, except for the initial occurrence of a Rising Threshold alarm, a CPU Utilization alarm will be generated only the when the sample value of the variable crosses the target threshold for the first time after having crossed the other threshold.

The diagram shown in Figure 23 illustrates how CPU Utilization trap events will occur once you have configured a CPU Utilization rising threshold. The startup condition for a CPU Utilization event is always predefined to be Rising.

CPU Utilization Event Generation

Figure 23: CPU Utilization event generation



The first CPU Utilization trap occurs at the initial sample value, since the value is above the CPU Utilization Rising threshold. If the initial value were below the Rising threshold, no event would occur.

The second event occurs at point X, because the sample value has fallen below the falling threshold, which is defined as 80% of the rising threshold value. The third event occurs at point A because the sample value is again above the Rising Threshold after having fallen below the Falling threshold. At point B the value again passes the Rising Threshold, but no alarm is generated because the value has not yet become less than the Falling threshold. Another Rising threshold alarm cannot occur until after a Falling threshold event has occurred, which happens at point Y. The next Rising threshold event happens at point C.

Note that in order to have any of these events cause an alarm in the EPICenter Alarm System, you need to define an alarm that responds to a CPU Utilization Rising Threshold or CPU Utilization Falling Threshold event.

- If you define an alarm based on the CPU Utilization Rising Threshold event, an EPICenter alarm will occur at the initial sample, and at points A and C. Because the alarm was defined to respond to CPU Utilization Rising Threshold events, the falling threshold trap events that occur at points X and Y do not trigger an EPICenter alarm.
- If you also define an alarm based on a CPU Utilization Falling Threshold event, then EPICenter alarms would be generated at points X and Y.

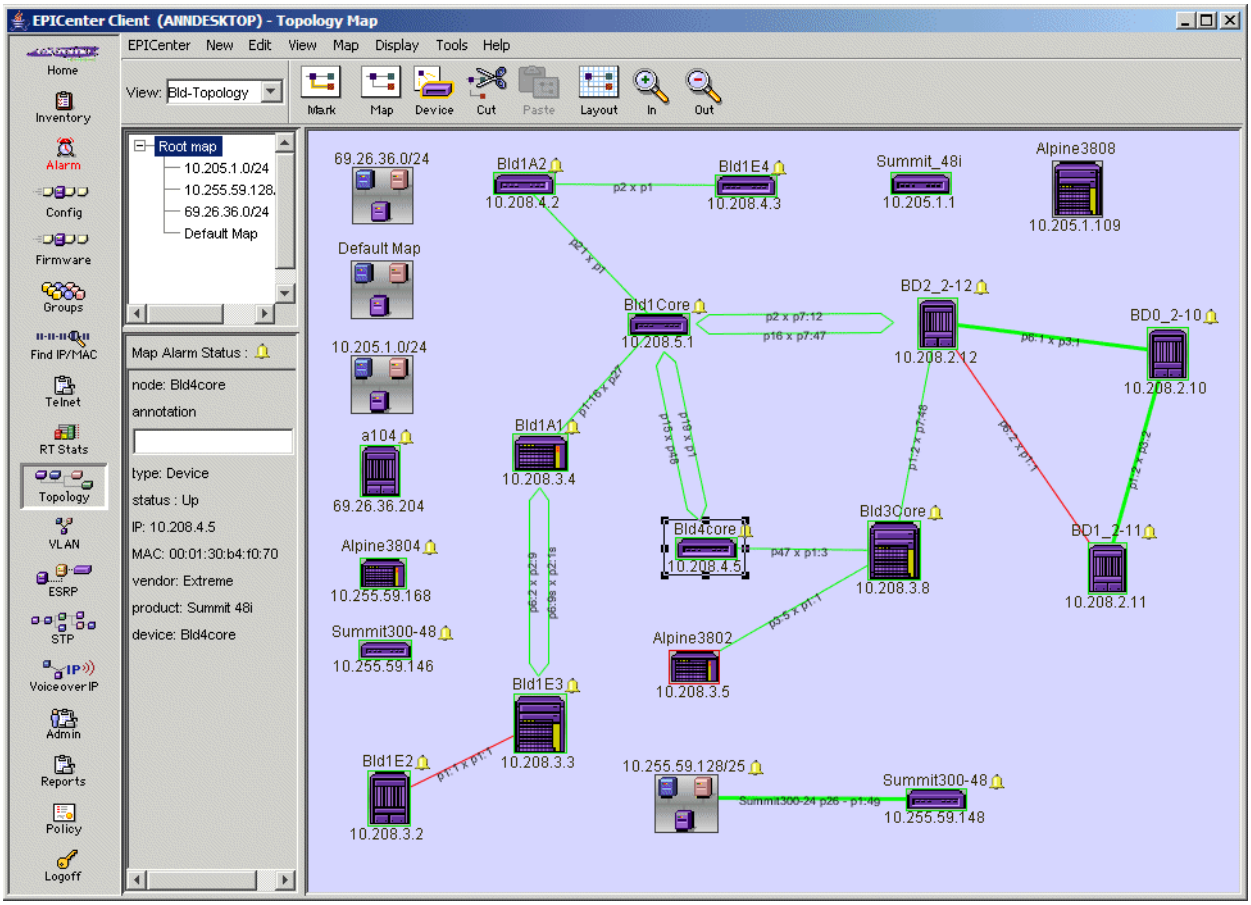
Using Topology Views

EPICenter topology views let you create visual representations of your network showing the devices, links between devices, and basic status of those devices and links, including link utilization statistics and VLAN membership and configuration information.

EPICenter automatically creates a default view with a set of network maps based on the IP addresses of the management interfaces in the devices on your network. You can create multiple additional Topology views to meet whatever needs you have. You can create Topology views that represent the physical topology of your network (buildings, floors, wiring closets and so on), the logical topology of your network (by operating divisions, departments, or workgroups) or by functional groupings (core devices vs. edge devices, ESRP devices, EAPS rings, and so on).

A Topology View consists of a root map and submaps. Within a given Topology view, devices can be represented only once, but the same devices can appear in multiple Topology Views—while the maps and submaps within a view are interrelated, Topology Views are independent of each other. This allows you to create multiple views of your network for different purposes.

Figure 24: Basic Topology Map



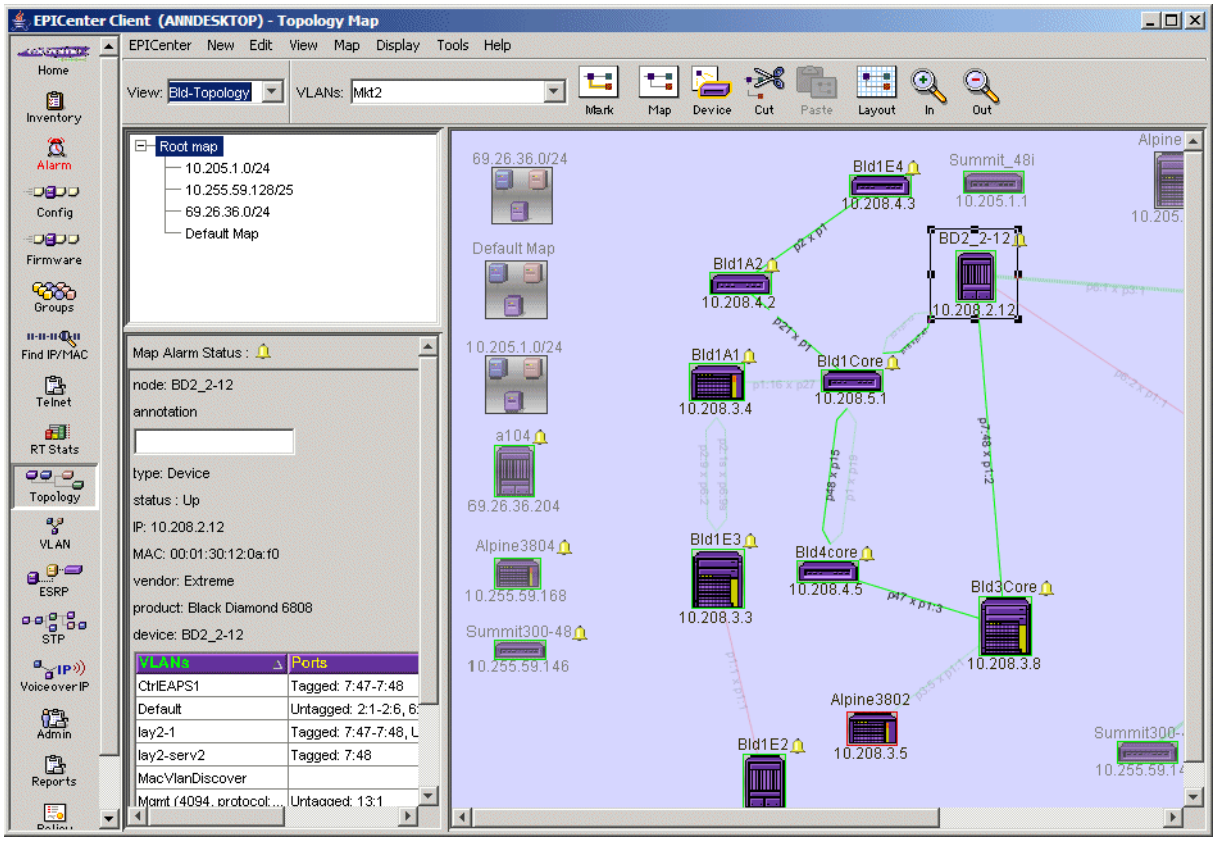
A basic topology map such as the example in Figure 24 shows you a variety of information about the status of your network:

- The border color of each device image indicates whether they are up or down
- The presence of an alarm icon indicates that at least one unacknowledged alarm has occurred on the device, or on a device in a submap, with the color of the icon indication the highest severity level of the unacknowledged alarms
- The color of the links between devices indicates the status of the link, and the width of the link indicates its bandwidth.

By selecting a node or link on the map, you can see additional information about the selected element in the Map Element description panel at the left of the map display.

You can optionally have EPICenter shows VLAN information about your network. Figure 25 shows an example of a map with VLAN information displayed for a selected VLAN.

Figure 25: Topology Map with VLAN information



In this mode, the map dims out all the links that are not involved in the selected VLAN. It also shows information about the VLANs for a selected device in the Map Element Description panel. You can even do some basic VLAN configuration from the Topology View in VLAN mode—such as adding links or edge ports to a VLAN.

Automated Map Creation vs. Manual Map Creation

EPICenter automatically creates the Default Topology View based on the devices in your EPICenter inventory database. It creates submaps based on the subnet structure of your network, and auto-populates the map with devices based on that structure. It also attempts to discover the links between devices using EDP, and places those on the map as appropriate. As new devices are added to the EPICenter inventory, they are automatically added to the default map (unless you have disabled the auto-populate feature for the default view).

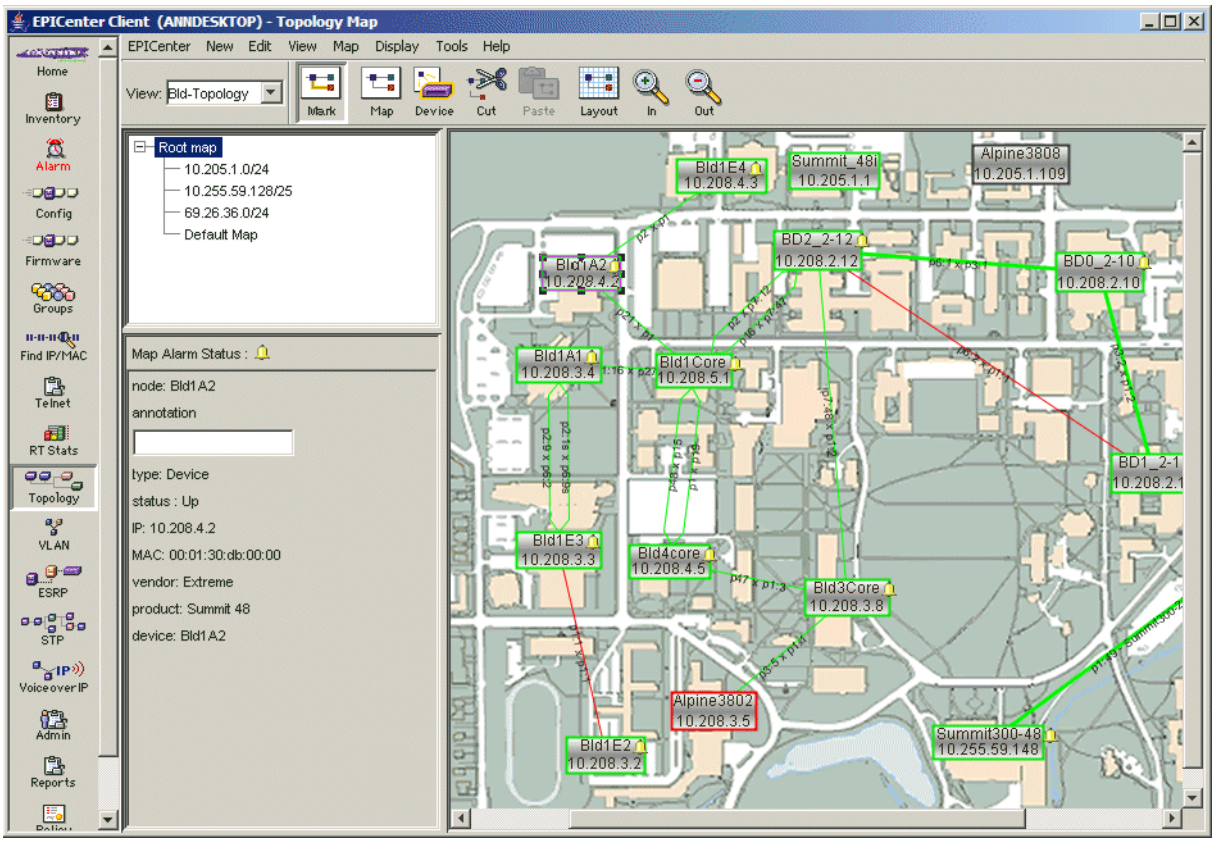
EPICenter cannot discover links between devices where EDP is not running (third-party devices, Extreme Networks devices with EDP disabled, or Extreme Networks devices running certain old versions of ExtremeWare). However, you can add user-defined links between devices to represent links that EPICenter cannot discover. Once you specify an endpoint (port) on each device for the link, EPICenter can display status for that link.

You can create new Topology Views to represent your networks in any way you want. You can have EPICenter auto-populate a view you create or you can select devices to add to your map individually. You can create and delete submaps, add, move and delete devices, create links, add annotations, give names and labels to your devices and so on.

Customizing the Look of Your Maps

In addition to determining the network elements that appear on your Topology maps, you can also customize the look of your maps. You can change the color of the map background or add a background image, control whether device names and icons are displayed or not, control the size and color of the text used for node annotations, and so on. Figure 26 shows a topology map with a campus map as a background image, and with device icons not displayed. EPICenter provides a few standard images, such as maps of the United States and Europe, and you can add images of your own as well.

Figure 26: Topology Map with VLAN information



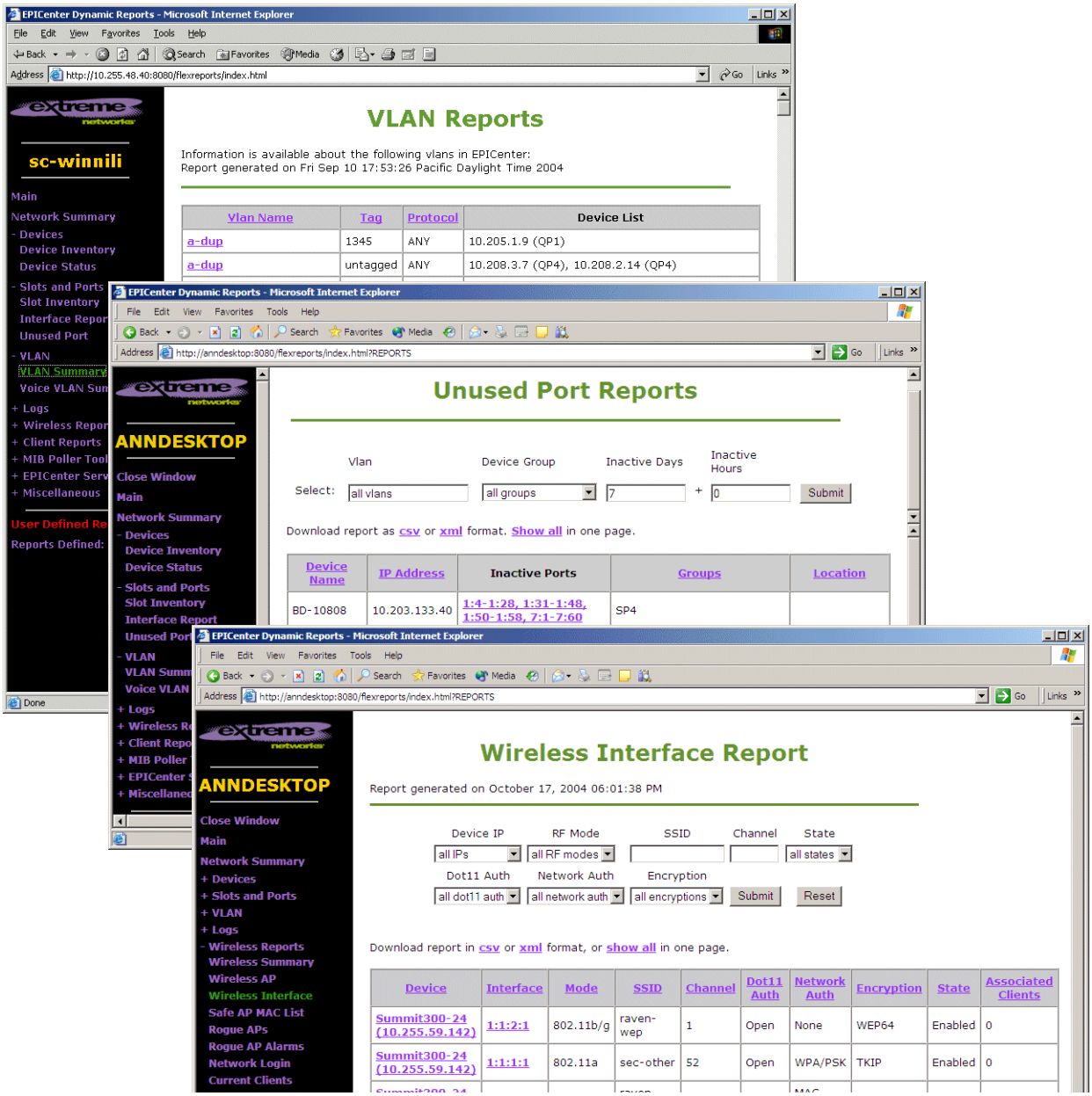
Using Basic EPICenter Reports

EPICenter provides a large number of reports based on the data in the EPICenter database. The Network Status Summary Report that appears when you first log into the EPICenter client is one example of these reports.

EPICenter reports are displayed in HTML in a browser window, even if you are running the EPICenter installed client. You must have a browser installed on your client system to be able to view reports. You can also view reports by logging directly into the Reports feature from a browser, without running the EPICenter client: just select the **View Reports** link from the EPICenter start-up page.

Figure 27 shows a few of the reports you can view through the Reports feature.

Figure 27: Examples of EPICenter reports



Most reports can be sorted in a number of ways, and many reports can be filtered to display only the data of interest, based on the types of information shown in the report. In addition, from some reports the displayed data can be exported to files in formats (csv or xml) that can be imported into other applications for analysis or display.

In addition to the Network Summary Report, EPICenter provides the following reports and tools:

Report Category	Report Name	Description
Main	• Extreme Networks eSupport Export	Exports EPICenter data for use by Extreme Networks technical support. Accessible from the Main reports page.
Network Summary Report	• Network Summary Report - Distributed Server Report	Summary status of the network, as well as version and path information about the EPICenter server. Status of distributed servers if Gold upgrade is installed.
Devices	• Device Inventory Report - Device Details Report - Power over Ethernet Report	Overview of devices known to EPICenter, by Device Group. From this report you can access the Device Details report, and additional subreports such as PoE information for devices that support PoE.
	• Device Status Report	Status of individual devices
Slots and Ports	• Slot Inventory	Inventory of cards installed in devices in the EPICenter database
	• Interface Report	Inventory of all ports on devices in the database
	• Unused Port Report	Summary of inactive ports by device including location, with subreports showing VLAN membership
VLAN	• VLAN Summary	Summary of all VLANs with device associations with subreports showing configuration details
	• Voice VLAN Summary	Summary of voice VLANs, with subreport showing phone and egress parts by device
Logs	• Alarm	EPICenter alarm log (more information available through Alarm Log Browser feature)
	• Event	EPICenter event log entries
	• Syslog	Syslog entries
	• Config Mgmt	Log of configuration management actions (config file uploads/downloads) and results
Wireless Reports	• Wireless Summary	Wireless status overview; links to supporting detail reports
	• Wireless AP	Inventory of Extreme Wireless Access Points
	• Wireless Interface Report - Wireless Port Detail	Inventory of wireless interfaces (radios), with a subreport on Wireless port details for a selected interface.
	• Safe AP MAC List	List of MAC addresses known to be from legitimate APs From this report you can add a list of MAC addresses to the Safe AP list, or delete addresses from the list.
	• Rogue APs - Rogue AP Detail	List of Wireless APs not on the Safe AP list, and not shown in the wireless AP report. From this report you can access the Rogue Access Point Detail Report, where you can add the AP to the Safe AP list, or disable the port if it can be uniquely identified.
	• Rogue AP Alarms	List of alarms due to the detection of rogue APs Enable/disable rogue AP detection here.
	• Network Login	List of network login activity by device
	• Current Clients	List of all current wireless clients detected, regardless of client state
	• Client History	Historical presentation of activity by wireless client
	• Spoofed Clients	List of clients with the same MAC address detected on different wireless interfaces
	• Unconnected Clients	List of wireless clients not in the data forwarding state

Report Category	Report Name	Description
Client Reports	• Network Login	List of network login activity by device
	• Current Clients	List of all current wireless clients detected, regardless of client state
	• Client History	Historical presentation of activity by wireless client
	• Spoofed Clients	List of clients with the same MAC address detected on different wireless interfaces
	• Unconnected Clients	List of wireless clients not in the data forwarding state
MIB Poller Tools	• MIB Poller Summary	Displays data in a MIB collection. Users with an Administrator role can start or stop a collection.
	• MIB Query	Provides an interface to query for the value of specific MIB variables. This is available only to users with an Administrator role. See “Using the MIB Poller Tools” on page 123 for more information.
EPICenter Server	• Server State Summary	Shows a variety of status information about the EPICenter server.
	• Debug EPICenter	Tools to aid in analyzing EPICenter performance. These are available only to users with an Administrator role. See“Using the EPICenter Debugging Tools” on page 132 for more information.
Miscellaneous	• Resource to Attribute	Shows all resources that include a specified attribute (from the Grouping Manager)
	• User to Host	Lists current set of user to host mappings, including primary IP address of the host

See the EPICenter online Help or the *EPICenter Reference Guide* for detailed information on what each of these reports shows.

3 Managing your Network Assets

This chapter describes how to manage and monitor your network assets. Topics include:

- Creating a complete network component inventory
- Importing inventory information using command line utilities
- Using Device Groups to organize and manage inventory
- Using Port Groups for monitoring critical network links
- Uploading inventory information to Extreme Networks for service and support
- Using Reports to view your device inventory

Creating a Network Component Inventory

There are several ways you can create an inventory of your network components:

- Use the EPICenter Discovery feature to automatically discover the devices on your network. YOu can then determine which devices to add, setting contact information for them as you do so.
- Add devices individually using the Add Devices and Device Groups dialog in the Inventory Manager
- Add devices to the inventory using a command line script

You may also want to create in advance a set of Device Groups so that you can assign the devices to the appropriate Device Groups as you add them. Or, you can add your devices initially into the Default Device Group, and then easily assign them to different device groups later.

Using Discovery to Find Network Devices

Using the Inventory Manager's Discovery feature lets you find all the devices on your network that are running SNMP agents. Once the devices have been discovered, you can then add them to the EPICenter inventory database, providing device contact information and assigning them to device groups as you add them. Thus, using Discovery you can configure and organize your device inventory in a single process.

You can tailor the discovery process to control the types of devices it will discover:

- You can restrict the discovery to only Extreme Networks devices (the default) or have it discover all MIB-2 compatible devices.

- You can restrict the discovery to devices running SNMPv1 (the default) or allow it to discover devices running SNMPv3 as well.

You can also control the range of IP addresses over which EPICenter will try to discover the devices it can manage:

- You can specify a single address or subnet specification, using wildcard characters as needed
- You can specify the start and end addresses of a range of IP addresses
- You can also use a subnet mask to modify the range of addresses to be searched.

Valid wildcard characters are *****, **?**, and **-** (dash):

***** acts as a wildcard for the entire octet (0-255).

? is a wildcard for a single digit (0-9).

- lets you specify a range for any octet. You can use this in more than one octet. Note that you cannot combine the dash with another wildcard in the same octet. The following are some examples of using wildcard characters in an IP address

10.203.0.*	polls 10.203.0.0 through 10.203.0.255
10.203.?.??	polls 10.203.0.0 through 10.203.9.99
10.203.0.1? or 10.203.0.10-19	both specify the same range: 10.203.0.10 through 10.203.0.19
10.203.0-2.10-30	polls 10.203.0.10 through 10.203.0.30 10.203.1.10 through 10.203.1.30 10.203.2.10 through 10.203.2.30

The subnet mask can also be used to specify a subnet not on the octet boundary: for example, specifying an IP address of 10.203.16.0 with a mask of 22 will expand to the range 10.203.16.1 - 10.203.19.254, a range of 1022 addresses.

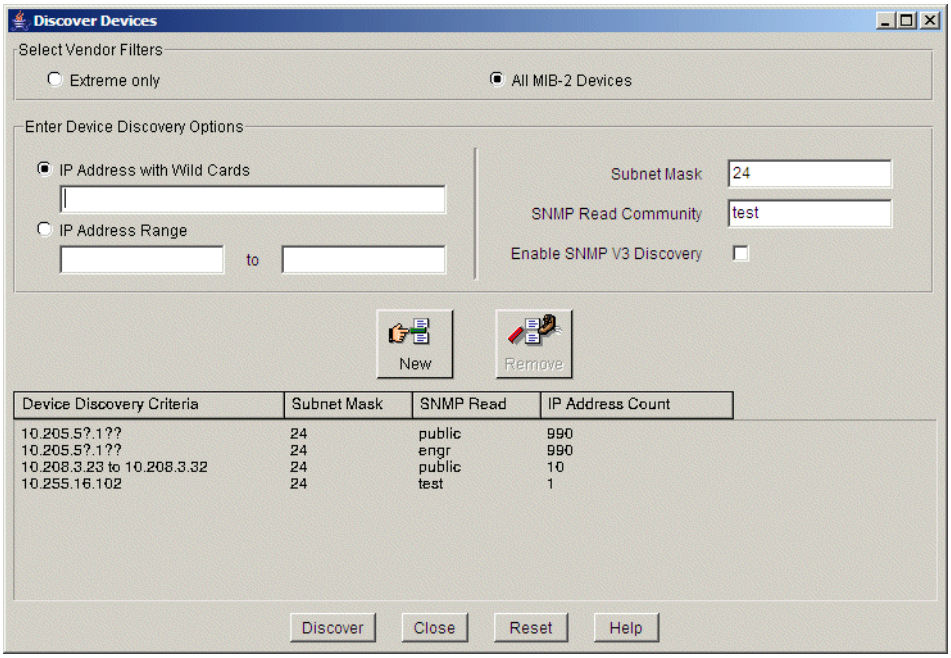
The ranges specified through the use of wild cards and the subnet mask interact in that the two specifications are combined with an “and” conjunction. This means that the more restrictive of the specifications will be the one to take effect.

IP addresses are processed prior to starting the discovery, and IP addresses that contain 255’s in the host portion are eliminated. This is based on the IP address as well as the subnet mask.

The EPICenter Discovery dialog lets you create a Discovery request that combines multiple discovery specifications. This means that within a single discovery operation you can have EPICenter discover devices in different address ranges, or search using several different read community strings, for example.

Figure 28 shows an example of a set of device discovery criteria that will all be used during a single discovery operation.

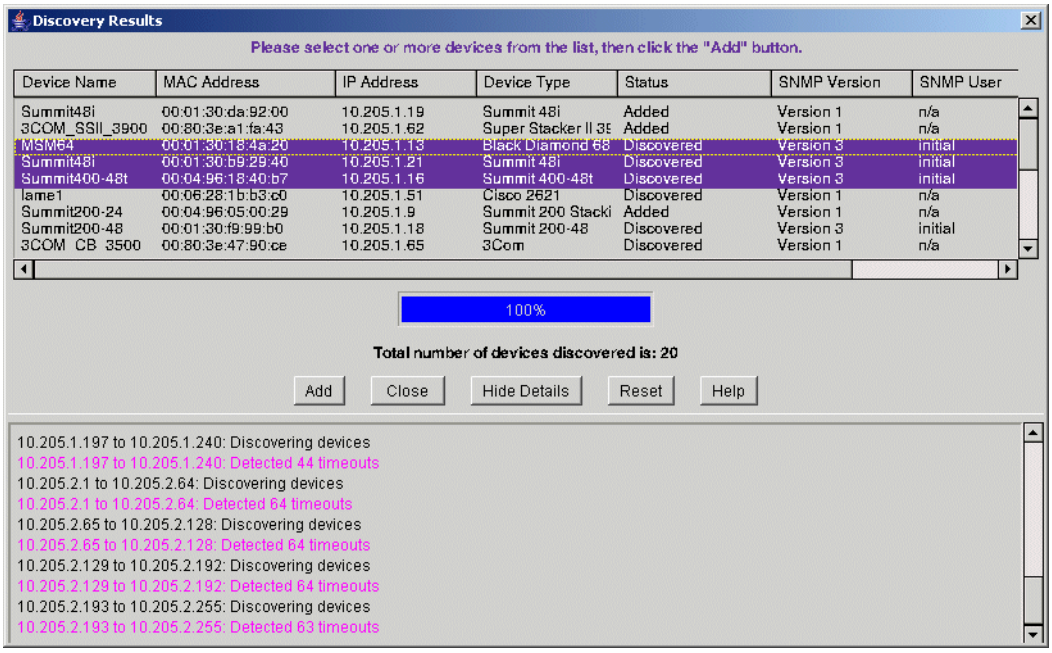
Figure 28: Device Discovery specifications



Once the discovery results have been returned, you can then select the devices you want to add the EPICenter inventory. Discovery does not automatically add any devices to the EPICenter inventory.

From the Discovery Results window, you can select individual or multiple devices to add to EPICenter's inventory database. When you add devices to the inventory, you must specify (or confirm) the device contact information for those devices. Thus, you need to select groups of devices to add that share the same contact information, as the same values are used for all devices in a selected set.

Figure 29: Discovery Results window


Discovery Results
Please select one or more devices from the list, then click the "Add" button.
Device Name
MAC Address
IP Address
Device Type
Status
SNMP Version
SNMP User
Summit48i 00:01:30:da:92:00 10.205.1.19 Summit 48i Added Version 1 n/a
3COM_SSII_3900 00:80:3e:a1:fa:43 10.205.1.62 Super Stacker II 3E Added Version 1 n/a
MSM64 00:01:30:18:4a:20 10.205.1.13 Black Diamond 68 Discovered Version 3 initial
Summit48i 00:01:30:b9:29:40 10.205.1.21 Summit 48i Discovered Version 3 initial
Summit400-48t 00:04:96:18:40:b7 10.205.1.16 Summit 400-48t Discovered Version 3 initial
lame1 00:06:28:1b:b3:c0 10.205.1.51 Cisco 2621 Discovered Version 1 n/a
Summit200-24 00:04:96:05:00:29 10.205.1.9 Summit 200 Stacki Added Version 1 n/a
Summit200-48 00:01:30:f9:99:b0 10.205.1.18 Summit 200-48 Discovered Version 3 initial
3COM CB 3500 00:80:3e:47:90:ce 10.205.1.65 3Com Discovered Version 1 n/a
100%
Total number of devices discovered is: 20
Add
Close
Hide Details
Reset
Help
10.205.1.197 to 10.205.1.240: Discovering devices
10.205.1.197 to 10.205.1.240: Detected 44 timeouts
10.205.2.1 to 10.205.2.64: Discovering devices
10.205.2.1 to 10.205.2.64: Detected 64 timeouts
10.205.2.65 to 10.205.2.128: Discovering devices
10.205.2.65 to 10.205.2.128: Detected 64 timeouts
10.205.2.129 to 10.205.2.192: Discovering devices
10.205.2.129 to 10.205.2.192: Detected 64 timeouts
10.205.2.193 to 10.205.2.255: Discovering devices
10.205.2.193 to 10.205.2.255: Detected 63 timeouts

You can perform multiple Add operations from the Discovery results window, so you can discover a wide range of devices in one operation, and then add them in small sets based on which devices use common contact information, or how you want to place them in device groups. For example, in Figure 29, a set of devices that all use SNMPv3 have been selected to be added in one Add operation.

Each time you add a set of devices, EPICenter updates the information shown in the discovery results section to indicate the devices that are now already in the database. The top two rows in the example in Figure 29 show devices that have already been added. The Discovery Results will continue to be displayed after an Add operation has finished, until you close the window.

When you click **Add**, EPICenter presents the default contact information and device group it will use, and gives you an opportunity to either confirm it or change it as appropriate. You can change what EPICenter uses as its defaults—see “Setting up Default Device Contact Information” on page 35, or refer to the online Help for the Discovery applet for more information.

If you want to add devices into specific device groups rather than into the Default device group, you must create those device groups before you do the discovery. If you do not have device groups set up ahead of time, however, you can easily create additional device groups and move your newly-added devices into them later. If you have devices already in the inventory database, you can add devices to a new device group as you create it.

Adding Devices Individually

If you want to add an individual device, and you know its IP address, you can simply add it through the interactive **Add Devices and Device Groups** dialog. The fields in this dialog will be pre-filled with the default contact information, so adding a device can be as simple as just typing its IP address. However, you can also change any of the device contact values as appropriate, as well as selecting the device group to which the device should be added.

Importing Devices Using the DevCLI Utility

If you have a large number of devices you want to add the EPICenter inventory, and you have there addresses and contact information available in machine-readable form, you can use the DevCLI command line utility to import device information into the EPICenter database. The devCLI utility provides a set of commands you can use to add, modify and delete devices and device groups in the EPICenter inventory database. The following is a brief summary of how you can use this utility to automate the import of a large number of devices into the EPICenter database. Appendix B, "EPICenter Utilities" provides detailed information on using these commands.

The `devcli add` command lets you add devices either individually, or from a text file that contains IP addresses. Through command arguments you can specify all the device contact information for the devices as well as the device group to which the devices should be added.

The device contact information specified in an add command is used for all the devices added by that command. So, as with adding devices from a Discovery, you may need to use multiple `devcli add` commands to add sets of devices that use different contact information.

You can also use the devcli add command to create device groups. If you want to add devices to a specific device group other than Default, the device group must exists before you add the devices.

The following is an example of a set of commands you could use to add devices to the EPICenter inventory database in specific device groups:

1. Create the needed device groups. (This also be done interactively through the EPICenter user interface):

   ```
   devcli add -u admin -g "Bldg 1" -g "Bldg 2" -g "Bldg 3"
   ```

   This command uses the default EPICenter login name "admin" and the default password.

2. Add the first set of devices to device group Bldg 1:

   ```
   devcli add -u admin -f devList1.txt -r read -w write -g "Bldg 1"
   ```

   This adds devices listed in the file devList1.txt, with read and write community strings specified. The default values set in EPICenter will be used for the other device contact values (such as the device login and password).

   The file `devList1.txt` must be a plain ASCII text file containing only IP addresses with one IP address per line, such as:

   ```
   10.205.0.95
   10.205.0.96
   10.205.0.97
   ```

3. Add a second set of devices from file `devList2.txt`, to device group Bldg 2 that uses SNMP v3 with the default SNMP v3 contact information:

   ```
   devcli add -u admin -f devList2.txt -t 3 -g "Bldg 2"
   ```

Making Device Contact Information Changes

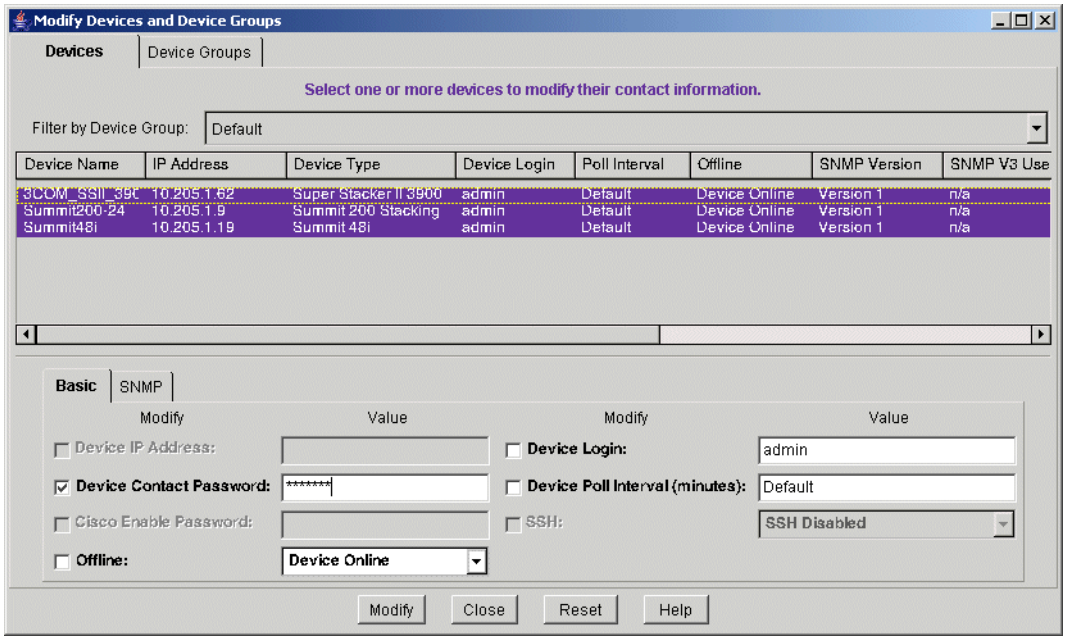
Periodically, for security purposes, you may need to change passwords, login users, or community strings on your network devices. If device contact information changes on a device EPICenter is managing, EPICenter will not be able to communicate with the device until you change the corresponding information in the EPICenter database.

You can change any of the device contact information kept for a device in the EPICenter database through the **Modify Devices and Device Groups** dialog in the Inventory Manager. If multiple devices use the same contact information, you can change the information for all those devices in a single operation (if they are members of the same device group).

In addition, you can change the device contact password (used for Telnet login) and the read and write community strings in EPICenter, and EPICenter will, at your option, also change them on the device. This means you can change basic device contact information from within EPICenter, and still maintain the ability to contact the device. You could then run a Telnet macro on the device to make changes to the other device contact settings.

To change contact information on multiple devices at the same time, from the **Modify Devices and Device Groups** dialog you select those devices in the device list, as shown in Figure 30. Fields that must be changed individually (such as the Device IP address and SSH) or fields that are not relevant (such as the Cisco Enable Password in this case) become unavailable.

Figure 30: Changing device contact information for multiple devices



When you change one or more of the settings that EPICenter can configure on the device, EPICenter displays a window asking if you'd like to make the change on the device as well as in the EPICenter database. If you change the device contact password and both community strings, the pop-up appears as shown in Figure 31.

Figure 31: Contact Information change dialog

Modify device contact information
Values will be modified in the EPICenter database.
EPICenter can also modify the following values on the device:
Device Contact Password
SNMP Read Community String
SNMP Write Community String
Modify device and database?
Device and Database
Database only
Cancel

You can change the value in the database only, or in both the database and on the device (or do neither). You might elect to make changes in the database only if the values had already been changed on the devices. If you are applying these changes to multiple devices, EPICenter will initiate the operation on multiple devices concurrently.

If you are changing contact information throughout your organization, you may want to also change the default contact information that EPICenter uses. See “Setting up Default Device Contact Information” on page 35 for more information about this.

Organizing Your Inventory with Device Groups

Device groups in EPICenter are very useful for grouping together devices with common characteristics so you can operate on them as a unit. Since you can put a device into multiple device groups, you can set up special purpose groups for a variety of functions.

For example, in the previous section, putting devices into device groups based on common contact information would simplify the process of doing bulk changes of contact information. You could just select the entire set of devices in the group and modify the information for all those devices in a single operation.

Another very useful function of device groups is to create groups for scoping alarms. To reduce load on your network and on the EPICenter server, you may want to limit specific alarms to a subset of your devices for which those events are critical. Using device groups for this purpose has several benefits.

- First, it simplifies the alarm definition process, especially if you plan to define multiple alarms that should all be scoped to the same subset of devices. If you don’t use a device group, you will have to add all the devices individually to the alarm scope over again for each alarm you create.
- Second, if you add device to the network that should be a member of this subset of devices, or if you remove a device, you can update the device group (as a single operation) and the change will immediately affect the scope of all alarms that use that device group. You will not need to modify any of the alarm definitions -- the scope will be changed automatically, as the alarm is scoped to the device group, not to individual devices.

The second point is one of the most powerful aspects of using device groups, and it applies to port groups as well (discussed in the next section). By using groups and then taking actions on the groups rather than on individual devices, you can simplify the overhead involved in adding or changing your network components.

Device groups can be useful in the following areas:

- Alarms: If an alarm is scoped on a device group, when the group membership changes, the alarm scope automatically reflects that change.
- Telnet macros: If a Telnet macro has a device group execution context, you can run the macro on all members of the device group by selecting the device group node in the Component Tree and executing the macro. Similarly, in the Macro Player, you can select a device group in the Component Tree, select all devices in the group, and run a macro on the complete set of devices.
- Bulk modify of device contact information: If you group your devices by the commonality of the device contact information, in the **Modify Devices and Device Groups** window, you can select the device group, select all devices in the set, and then change device contact information for all the devices in the group in a single action.

Monitoring Critical Links with Port Groups

As with devices, you can also organize ports into groups using the Grouping Manager. Port groups can include ports from many different devices, and can be used as the scope for alarm definitions, as well as in the Real-Time Statistics applet to monitor utilization and error statistics on the ports in a group.

As an example, you might create a port group that includes the EDP ports (uplink ports) from a set of core devices in your network. You can then use the Real-Time Statistics applet to monitor the utilization and errors for those ports as a single display, even though the ports in the port group exist on different devices in your network. You could also define a critical alarm triggered by an SNMP Link Down event that has the port group as its scope. Then if one of the uplink ports goes down, a critical alarm will be triggered. However, if other ports on those same devices go down, they will not trigger the alarm.

Port groups are created in the Grouping Manager rather than the Inventory Manager. The ports in a group can be a mix of port types and can come from many different devices. For example, a port group made up of EDP ports might contain one port from each of many different devices.

Figure 32: A port group defined in the Grouping Manager

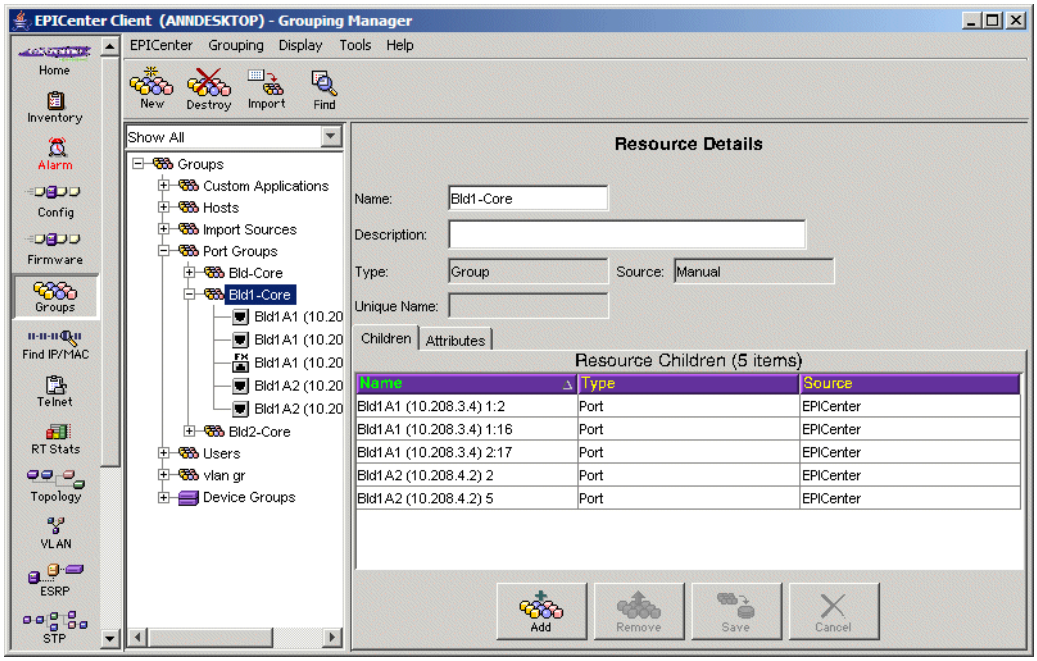
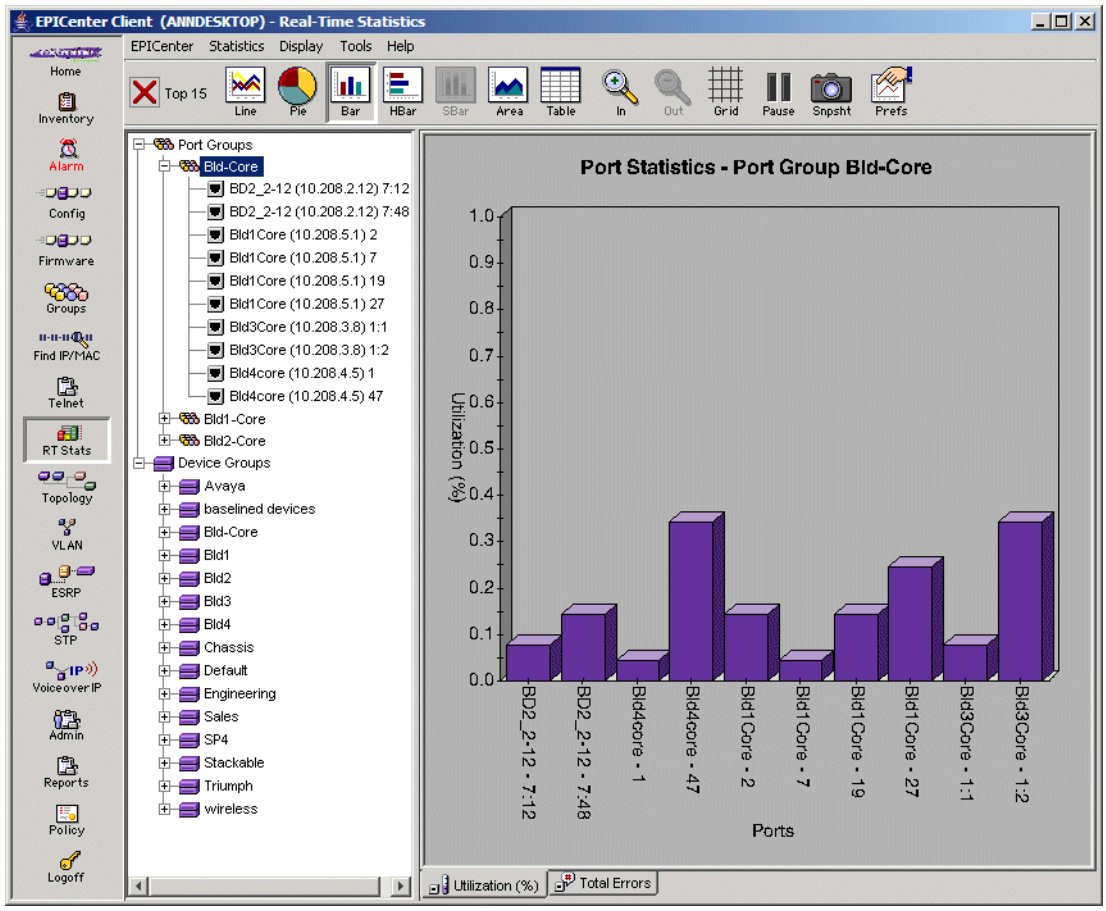


Figure 32 shows a port group as defined in the Grouping Manager for the uplink ports on the core devices in a specific building.

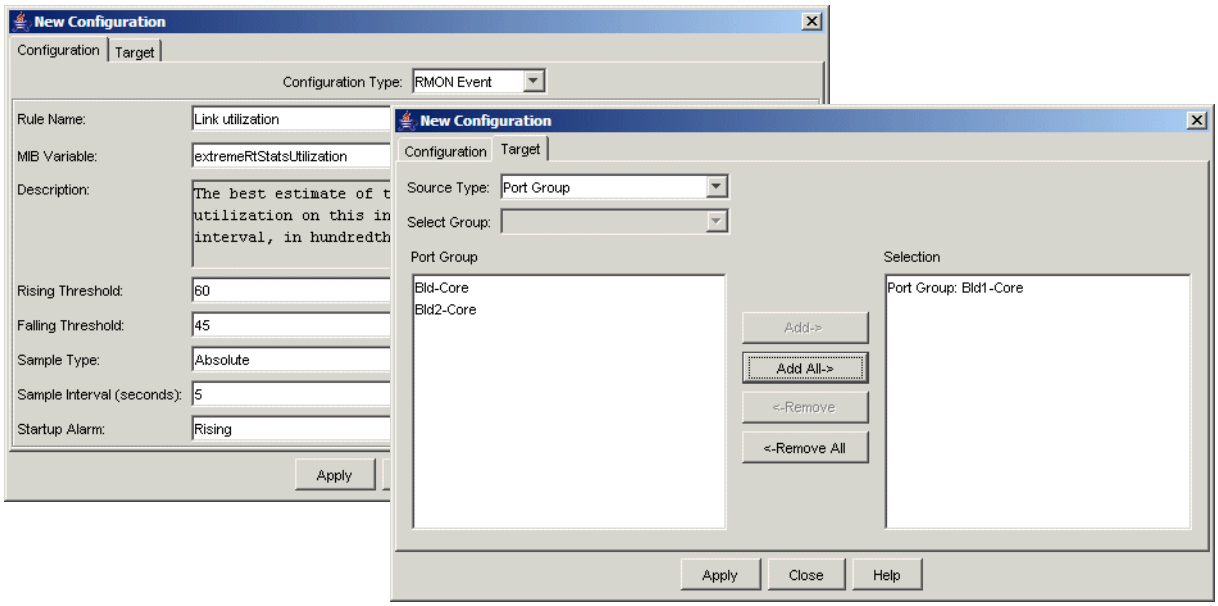
Figure 33 shows a utilization chart for the ports in the same port group. Even though the ports are on different devices, they can be grouped into a single statistical display, which makes it very easy to monitor the status of these critical links.

Figure 33: Utilization statistics for ports based on a port group



Using this same port group as the scope, you could define an RMON threshold rule for link utilization (for MIB variable `extremeRtStatsUtilization`) that would generate a trap when utilization exceeded some percentage you define on any of the ports in the port group. Figure 34 shows an example of how such a rule might be defined. You would then use this threshold rule to define an alarm, also scoped to the same port group

Figure 34: An RMON threshold rule for port utilization scoped on a port group



You could create similar port groups for load-shared ports, for example, or for the ports connecting to critical servers in your network.

Inventory Reports

The EPICenter Reports feature provides HTML reports on many aspects of the devices in the EPICenter database.

You can view Reports by clicking the **Reports** icon in the Navigation Toolbar from the EPICenter client, or you can view Reports directly from a browser without needing to load the EPICenter client—you can select the **View Reports** link from EPICenter's browser start-up page.

The Reports feature includes the following reports on the inventory of devices, slots and ports in the EPICenter database:

- **Device Inventory Summary** listing the Extreme Networks devices in a device group, or of a specific device type, including the MAC address, serial number, and current image on the device. From this report you can view a detailed report for an individual device. If you view the summary by device type, it also tells you what device groups each device belongs to.
- **Slot Inventory Summary** listing the modules installed in Extreme Networks devices, including the device in which the module is located as well as the card serial number.
- Port Inventory reports (**Interface Report** and **Unused Ports Report**), showing the ports on Extreme Networks devices in the database.
  - The **Interface Report** shows the administrative, operating, and FDB polling status, configured and actual speeds, as well as the device on which the port appears. It shows all ports on your network by default, but can be filtered by criteria such as IP address, configured or actual speed, status and so on.
  - The **Unused Ports Report** shows the inactive ports in the network, which can be filtered by device group, VLAN, or length of time the ports have been inactive. You can view detail reports

by device, which show the port type, VLAN membership (if any) and length of time the port has been inactive, for the inactive ports on a device.

Each of these reports can be exported in csv or xml format.

Uploading Inventory Information to Extreme Networks

If it happens that you need to work with Extreme Networks' Technical Assistance Center (TAC), the TAC personnel may need information on your devices in order to provide the appropriate assistance. From the EPICenter Reports main page you can export device inventory information to a file in a format that you can then upload to Extreme Networks.

To create a report suitable for upload to Extreme Networks, select a device group (or "all groups") from the drop-down field at the top of the Main Reports page, and click **Export**.

4 Configuring and Monitoring Your Network

This chapter describes how EPICenter can help you configure, monitor, and manage the components of your network on a network-wide basis. Topics include:

- Configuring multiple devices concurrently using user-defined Telnet macros
- Network-wide configuration of VLANs
- Monitoring network configuration through graphical and HTML-based displays

Scalable, Concurrent Multidevice Configuration

In a large network, the burden of configuring, monitoring and managing your network devices one-by-one can become overwhelming, especially when a global configuration change needs to be made across a large sets of devices (creating a new network-wide VLAN, for example, or globally enabling or disabling certain functionality). EPICenter provides several ways to accomplish scalable, concurrent configuration of multiple devices.

An important feature of EPICenter is its support of Telnet macros, which provide a way to make configuration changes on multiple devices concurrently with minimal administrator intervention. Through the EPICenter Telnet applet, you can create your own Telnet macros to perform device configuration actions, and then have EPICenter run those macros on multiple devices. Due to multi-threading EPICenter can execute a macro on multiple devices concurrently, significantly reducing the time it takes to implement a configuration change across many devices.

Telnet macros are also useful for automating standard configuration tasks that can be executed in the same way over and over as needed. For example, when new devices are added to the network, a macro can be run on the new device to implement the configurations that are standard across all devices on the network, or that are standard to devices of a certain type.

Once a macro has been created, it can be scoped so that it can be run on a device (or all the devices in a device group) without requiring access to the Telnet applet itself. This allows an EPICenter administrator to restrict access to EPICenter's Telnet applet (and thus direct Telnet access to a switch) to a select group of users, while still allowing a larger set of EPICenter users to perform pre-defined switch configuration tasks. This means that an administrator can abstract some of the common CLI commands, and give non-administrator users controlled access to a subset of the CLI without enabling access to the entire spectrum of CLI capabilities.

User-Defined Telnet Macros

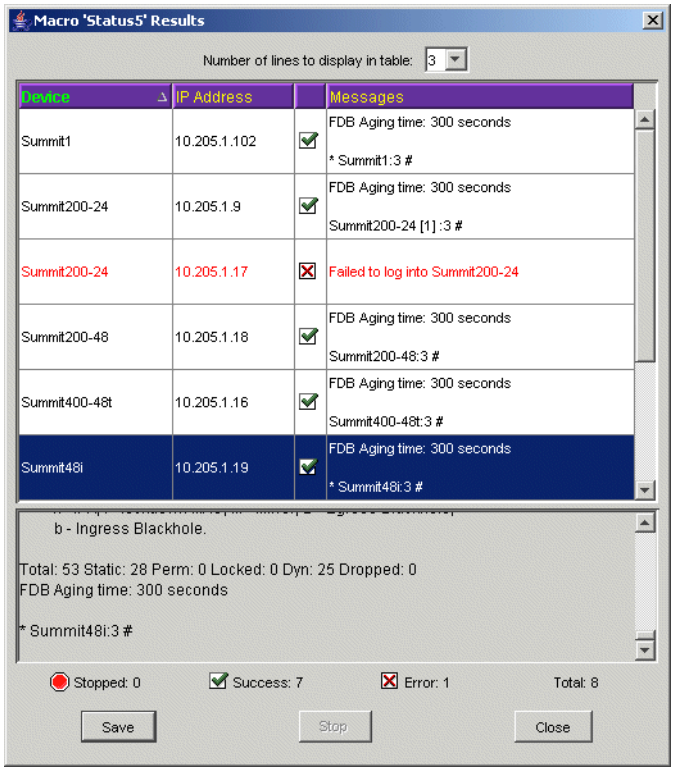
The Telnet applet provides both a Macro Editor and a Macro Player function, in addition to allowing interactive Telnet access to individual devices. Telnet macros can be created in either the Macro Player or the Macro Editor. You use the Macro Editor to create and save macros that are intended to be re-used.

In the Macro Player, you can enter a macro (or load a saved macro) and run it on a selected set of devices, but you cannot save the macro. The Macro Player function is provided primarily to enable macros to be run on a one-time or ad-hoc basis. You might use the Macro Player to enter a set of commands to be run on several devices at the request of Extreme Networks' Technical Assistance Center to help in diagnosing a configuration problem, for example.

Even though EPICenter can execute a macro concurrently on multiple devices, it still logs the responses and results separately for each device, and displays each in their own message area them in a tabular-style view so an administrator can easily monitor the configuration process to ensure that the changes are implemented successfully on all devices in the set. Results can be saved either as individual results files, or in a single file with results for all the devices in the set (useful if you need to send a set of results from multiple devices to someone such as Extreme Networks' Technical Assistance Center for review).

Figure 35 shows how the results from macros run on multiple devices concurrently are displayed, with the results from each device appearing in its own row. A row can be selected to display the complete set of results for that device, as is the case with the last device in the example.

Figure 35: Telnet macro results for multiple devices



Creating Telnet Macros for Re-Use

In the Macro Editor you can create user-defined variables that can then be used in the macro to allow run-time input of information (for example, a VLAN name) to the running macro. The Macro Editor also provides a set of system variables for parameters such as the device IP address, device name, date, time, port index, EPICenter server IP address, and so on. When the macro is run, these variables are replaced with actual values from the devices on which the macro is being run.

Example 1: A Macro to Configure EPICenter as a Syslog Server on a Device

One example of a macro you would re-use is a macro to configure EPICenter as a Syslog server for your Extreme Networks switches. You could create and save a macro that used a system variable to specify the EPICenter server's host name or IP address. To configure EPICenter as a syslog server with facility level local0, you could create the following macro:

```
config syslog add $serverIP local0
enable syslog
```

Once you've saved this macro, any time you want to configure EPICenter as a Syslog server on a switch, you just need to run the macro on that device. When the macro runs, the EPICenter server will substitute its own IP address for the `$serverIP` variable in the `config syslog` command.

Using Interactive CLI Commands in a Macro

For interactive commands used in a command macro, you need to supply the response to the command in a separate line. The following examples illustrate usage of some of these commands.

- To create a user account with the name "joesmith" and a password of "2joe3," enter the following commands:

  ```
  create account user joesmith
  2joe3
  2joe3
  ```

  NOTE

  If you type a command that requires a password, you need to enter the password twice. In a command macro, the first "password" sets the password, and the second "password" confirms the password.

- To use the `save` command to save a configuration to the switch, enter the following commands:

  ```
  save
  yes
  ```

- To delete a user-defined STPD domain (stpd2) from the switch:

  ```
  delete stpd2
  yes
  ```

- To reboot the switch:

  ```
  reboot
  yes
  ```

Example 2: A Macro to Configure a New Switch

Another example of a re-usable macro would be a macro to configure new network devices with the existing network configurations for specific VLAN, ESRP, STP or other customizations. This example uses user-defined variables to enable the input of specific port and IP address information.

```
create vlan sales
config sales add port $salesVlanPorts
config sales ipaddr $salesVlanIP
enable ipforwarding
enable esrp sales
enable edp ports all
config ospf add vlan sales
enable ospf
save
yes
```

`$salesVlanPorts` and `$salesVlanIP` are both user-defined variables. When the macro is run on a device, EPICenter prompts for the values of the two variables. It uses as the prompt the description you entered when you created the variable. Note that the save command requires a confirmation, which must be included in the script.

Once this macro has been saved, you can run it on each new device that is added to the network. You could also designate an execution context and an execution role for this command so that non-administrator users could run it on a new device to accomplish this specific set of configuration changes without having access to the Telnet applet and the full CLI.

Creating Macros to be Run From a Menu

Saved macros can be run from outside the Telnet applet, if they are given an execution context. They can appear under the Macros sub-menu, accessed from a right-click pop-up menu or from the Tools menu in many of EPICenter's applets. This means that users who do not have access to the Telnet applet (users with a Monitor role, for example) can still execute selected Telnet commands on network devices. A network administrator can create a set of Telnet macros to do common tasks and configure the macros to specify what users roles should be able to run those macros.

In the Macro Editor you can specify an execution context and execution roles for a macro. These allow you to create a macro that can be run outside of the Telnet applet.

- The execution context of a macro determines the type of components on which the macro can be run: ports, devices or device groups. For example, if you created a macro to add a port to a VLAN you would give it a port execution context. This means that the macro would be available from the Macros sub-menu only when a port is selected in the Component Tree. It would not be available when a device or device group is selected.

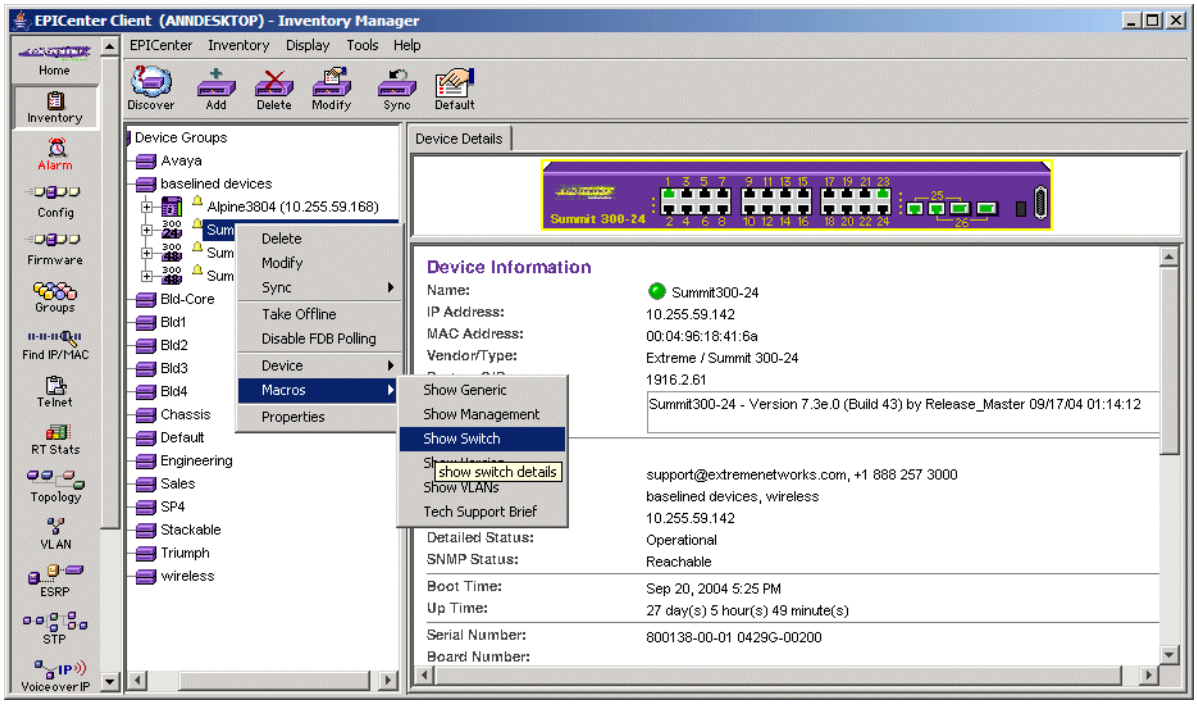
  Similarly, a macro with a Device execution context will be available only when a Device is selected. A macro with a Device Group context will run on all devices of a selected Device Group. A macro can have multiple execution contexts, if appropriate.
- An execution role defines which users can execute a macro. When you create a macro you can select which roles will have access to the macro—users whose roles are specified as execution roles will see the macro in the Macros sub-menu. Users whose roles are not included will not have the macro available. For example, if only Administrator and Manager roles are selected for a macro, then users with a Monitor role will not see that macro on the Macros sub-menu.

NOTE

The execution context and execution roles only affect how Telnet macros appear in menus outside the Telnet applet. Any user who has access to the Telnet applet can run any macro in any context.

Figure 36 shows an example of a set of Telnet macros available from the Macros sub-menu of a right-click pop-up menu. These macros have a Device execution context and thus are available on the Macros menu when a device is selected in the Component Tree.

Figure 36: Telnet macros available from the Macros sub-menu



The execution context and execution roles interact in that a macro will be available to a user only if the macro matches the execution context of the selected component (Device Group, Device, or Port) *and* the user's role has been included as an execution role defined for the macro.

If you do not specify any execution role at all for the macro, that macro will not be available for execution outside of the Telnet applet. In that case, only users who have access to the Telnet applet will be able to execute the macro, as it will be available to be run only from within the Macro Player.

Role-based Telnet Macro Execution

Role-based macros allow a network administrator to script certain configuration or status-display functions so that they can be performed by EPICenter users who should not have unlimited Telnet access to a device.

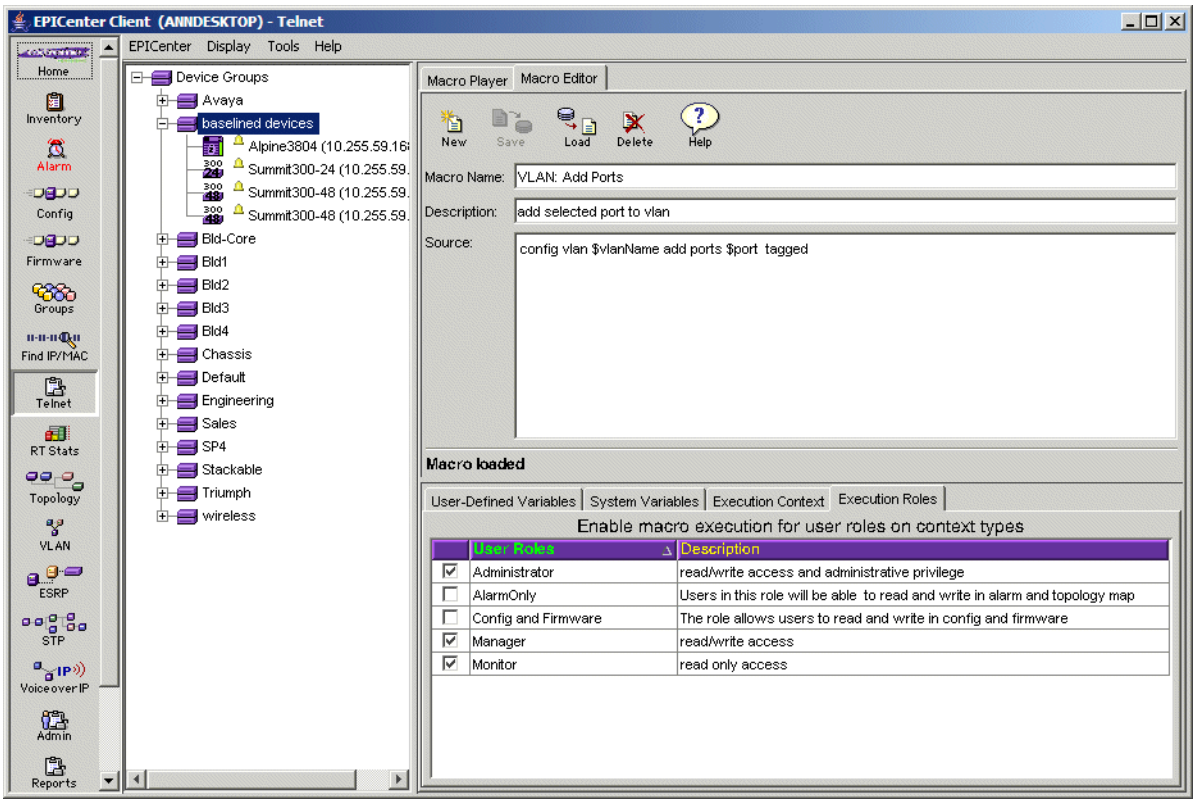
For example, a network administrator may want to allow an assistant to run macros that add the standard configuration settings to devices newly added to the network (as in the Example 2 on page 80) but not have Telnet access otherwise. The administrator could create a user role for his assistants that does not allow access to the Telnet applet. However, when creating the new device configuration macro, he would specifically allow the assistant role as an execution role for this macro. Any of his

assistants logged in with the assistant role could configure a new device without needing access to the Telnet applet.

Another common case would be allowing users with a read-only access role, such as the Monitor role, to run `show` commands of various sorts on devices on the network for troubleshooting read-only.

Figure 37 shows a Telnet macro in the Macro Editor, with several execution roles selected. The selection indicates that this macro will be available to users with Administrator, Manager, and Monitor roles, but not to users with AlarmOnly or Config and Firmware roles. (The AlarmOnly and Config and Firmware roles are user-defined roles.)

Figure 37: A Telnet macro with selected execution roles



Note that if you add a new role to EPICenter after you have created your Telnet macros, that role will *not* be included in the execution roles for your macros. If you want users with your new role to be able to execute your macros, you must return to the Macro Editor and modify (and re-save) the macros to include the new role.

Network-wide VLAN Configuration

EPICenter provides a number of features that enhance an administrator's ability to manage VLANs on the network. As VLANs span multiple devices, a network-wide view of VLAN configurations provides many benefits. Through EPICenter, VLANS can be managed in several ways:

- EPICenter's VLAN Manager supports network-wide, scalable, multidevice configuration of VLANs. It provides a network-wide view of all VLANs on all devices managed by EPICenter, which you can display either by switch (showing all the VLANs configured on a switch) or by VLAN (showing all

the switches with ports in the VLAN). The VLAN Manager also provides a graphical user interface for creating new VLANs and adding and removing device ports to or from an existing VLAN. Due to multi-threading, EPICenter can perform a VLAN configuration on multiple devices concurrently, rather than having to configure each switch in a VLAN one at a time.

Once you add a device and port to the VLAN, you can have the VLAN Manager check to see if connectivity exists between the new device and port and all the other members of the VLAN. If additional ports are needed to establish a path to another member of the VLAN, EPICenter will recommend the devices and ports to be added to the VLAN, and can add them to the VLAN if you accept the recommendation.

- EPICenter's Topology views can be used to show a topological view of the VLANs on your network. It will show links in a VLAN that are misconfigured (where the VLAN is configured on one side of a link but not the other). In addition, from a Topology map you can select links to add to a VLAN, or you can select a device, and add selected edge ports on that device to a VLAN that exists on the device.
- The use of Telnet macros enables standard VLAN configurations to be easily configured on multiple devices without extensive administrator intervention. This is particularly useful for configuring VLAN settings in a repeatable way on new devices that are added to the network.
- EPICenter's VLAN reports also provide information on VLAN membership, in a form that can be printed out if desired.

See Chapter 5, "Managing VLANs" for a more detailed discussion of EPICenter's capabilities for managing VLANs.

Graphical and HTML-based Configuration Monitoring

A number of EPICenter applets can be used to monitor different aspects of your network configuration on a network-wide basis:

- The Topology applet monitors and displays layer 1 EDP connectivity between devices. It shows information about link bandwidth and endpoint configuration, as well as the link status (up, down, or unknown). It also identifies links configured for load sharing.

  As an option, if RMON is enabled for your network devices, the Topology applet can show usage statistics for the links on a map. Note that for RMON statistics to appear on a map, three conditions must apply:

  — RMON must be enabled on the switches shown on the map

  — RMON data collection for Topology must be enabled (this is a Server Property configured in the Admin applet, and by default is enabled).

  — RMON statistics must be enabled for the specific map (this is enabled through the Map properties)

  Note that if you enable the display of RMON statistics on a map, this could add extra load to your system due to the additional data polling.

  The Topology applet can also be used to show VLAN information for links and devices. This is discussed further in Chapter 5, "Managing VLANs".
- The STP Monitor displays network-wide multi-device views of every STP domain. You can view information down to the state and configuration of every device port in each STP domain.
- The ESRP Monitor shows similar information network-wide for ESRP instances—the configuration of state of every device in each ESRP instance.

- The EPICenter Reports feature provides a large number of HTML-based reports that can be used to monitor network configuration details. These reports are tabular in nature, but they can be printed out, and in some cases they can be exported to a file in a format that then be imported into another application for analysis.

5 Managing VLANs

This chapter describes how to configure, monitor, and manage VLANs. Topics include:

- Graphically configuring and monitoring VLANs
- Scalable multidevice network-wide VLAN functionality
- Network-wide VLAN membership visibility
- Displaying VLAN misconfigurations with Topology maps

EPICenter provides a number of features that greatly simplify the management of VLANs on your network. Using EPICenter you can monitor and configure VLANs on a network-wide basis, rather than one device at a time. EPICenter automates the addition and deletion of device ports for the VLAN being configured, and supports scalable, multi-device VLAN configuration, which speeds the process of implementing VLAN changes across multiple devices.

Graphical Configuration and Monitoring of VLANs

EPICenter provides two facilities for configuring and monitoring the VLANs on your network through a graphical user interface — the VLAN Manager and the Topology Views. Both provide graphical user interfaces that let you view the VLANs on your network from several different perspectives on a network-wide basis.

The VLAN Manager provides a comprehensive network-wide view of all VLANs on all devices managed by EPICenter, which you can display either by switch (showing all the VLANs configured on a switch) or by VLAN (showing all the switches with ports in the VLAN). The VLAN Manager also provides a graphical user interface for configuring many aspects of a VLAN. With multi-threading, EPICenter can perform a VLAN configuration on multiple devices concurrently, rather than having to configure each switch in a VLAN one at a time. With the VLAN Manager you can:

- Create and delete VLANs
- Add or remove ports from existing VLANs
- Modify a VLAN's IP address
- Enable and disable IP Forwarding
- Create and modify the protocol filters used to filter VLAN traffic

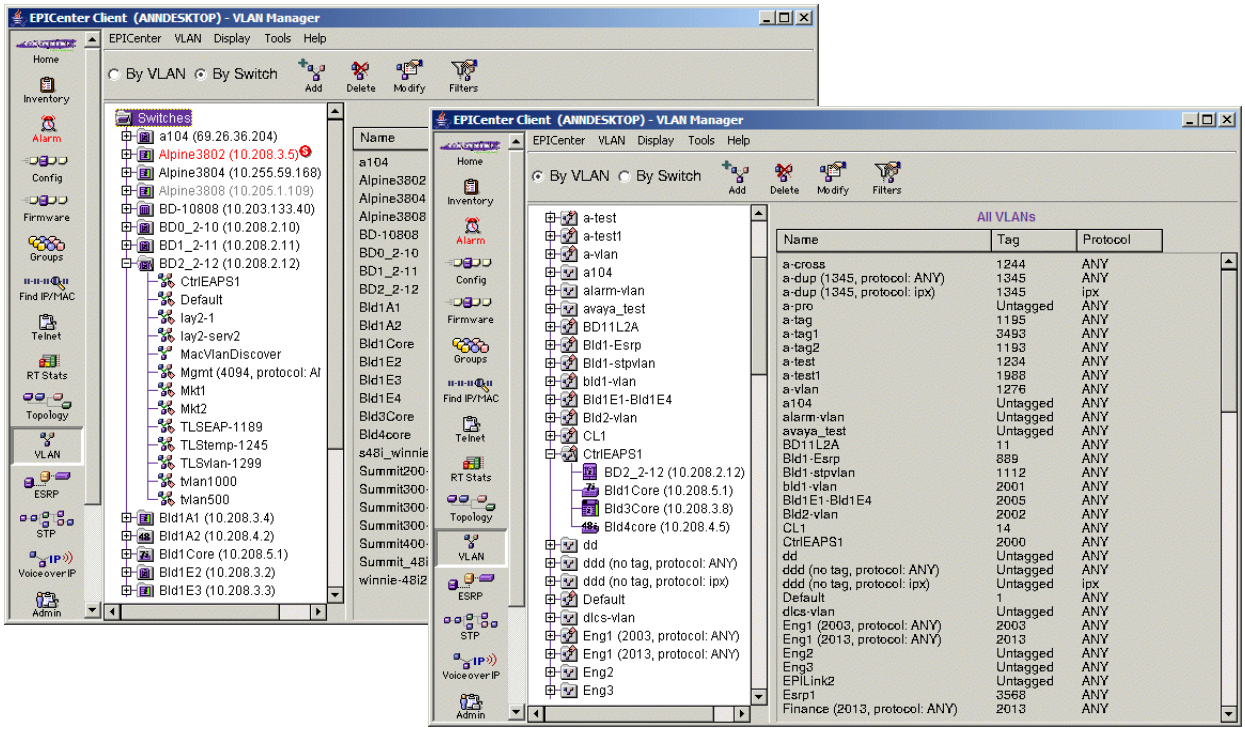
The Topology applet, on the other hand, lets you view your VLANs from the perspective of the network interconnections. By selecting a VLAN you can quickly see the device connectivity enabled by the VLAN. Through Topology Views you can:

- Identify misconfigured VLAN links
- Select links to add to an existing VLAN or create a new VLANs using the selected link
- Add edge ports to a VLAN that exists on a selected device

Network-wide VLAN Membership Visibility

The VLAN Manager provides a comprehensive view of all the VLANs on your network. The VLAN Manager's main view shows you a summary of all VLANs on your network, either by switch or by VLAN.

Figure 38: Viewing VLANs by switch or by device in the VLAN Manager



By selecting an individual VLAN you can see all the devices and ports that are included in the VLAN.

By selecting an individual device, you see all the VLANs on the device, along with information about the tag, IP address, protocol, and the ports that belong to each VLAN. You can also view similar information about the VLANs on a device from the VLAN tab of the Device Properties display for the device.

A Topology View with VLAN information displayed shows you, for a given VLAN, the devices on the map that have the VLAN configured, and the links that connect the VLANs on those devices. Figure 39 shows an example of the display for a selected VLAN.

By default, VLAN information is not shown in the normal view of a topology map. To view VLAN information on a map you must enable the VLAN information display:

1 From the Display menu, select VLAN Information. This displays the VLAN field on the Topology map Toolbar.

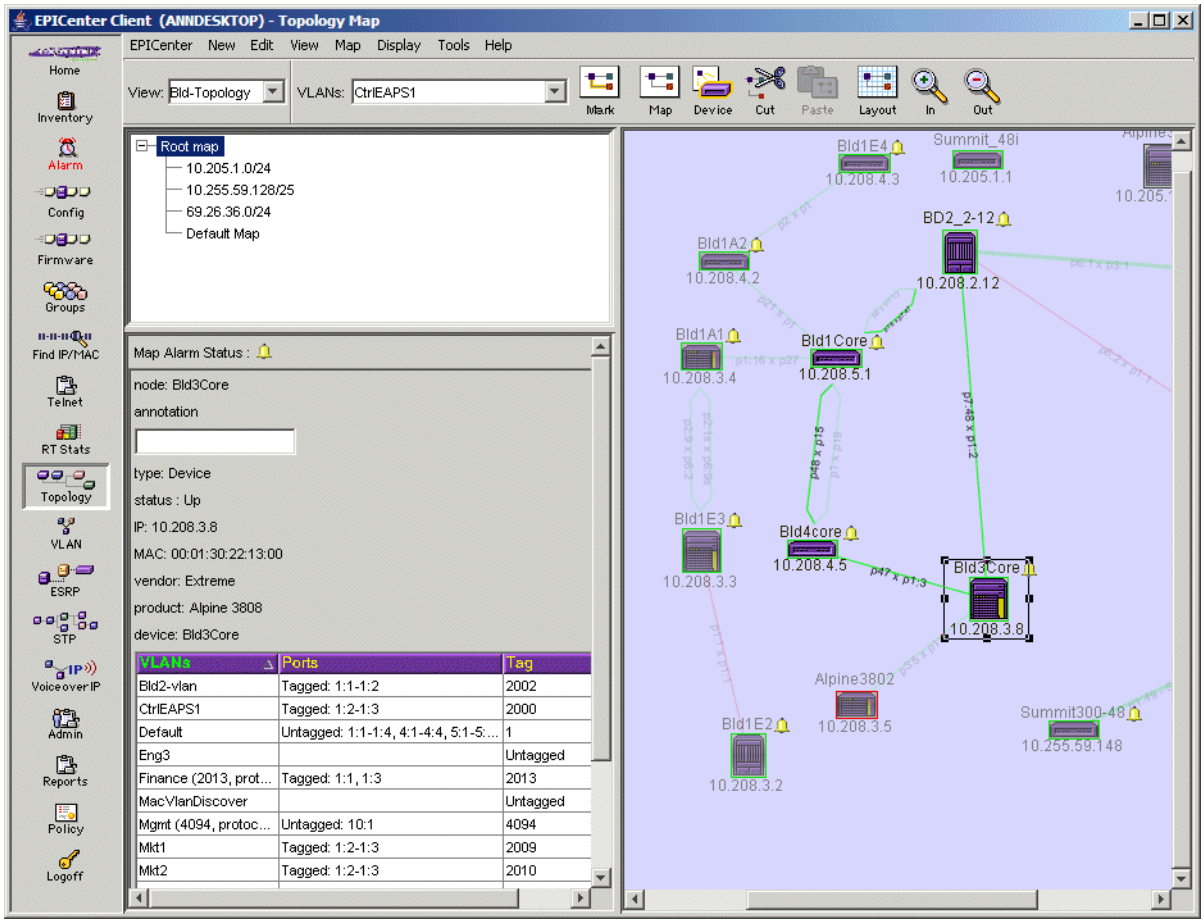
NOTE

*The VLAN field displays all VLANs on any **link** shown on the map. It does not necessarily display all VLANs on the devices on the map.*

2 Select the VLAN you want to view from the drop-down list in the VLAN field.

The devices and links that are not part of the VLAN are dimmed on the map so that the devices and links in the selected VLAN are visible.

Figure 39: Displaying a VLAN on a Topology map.



Selecting one of the devices in the topology map shows, in the Map Element Description panel at the left, the VLANs on any of the links on the device, along with the ports in each VLAN and the VLAN tags. It does not necessarily show *all* VLANs on the device. You can view all VLANs configured on a device through the VLAN Manager applet.

Selecting a link in the VLAN shows you basic information about the two endpoints of the link and lists the VLANs that are configured on both endpoints of the link.

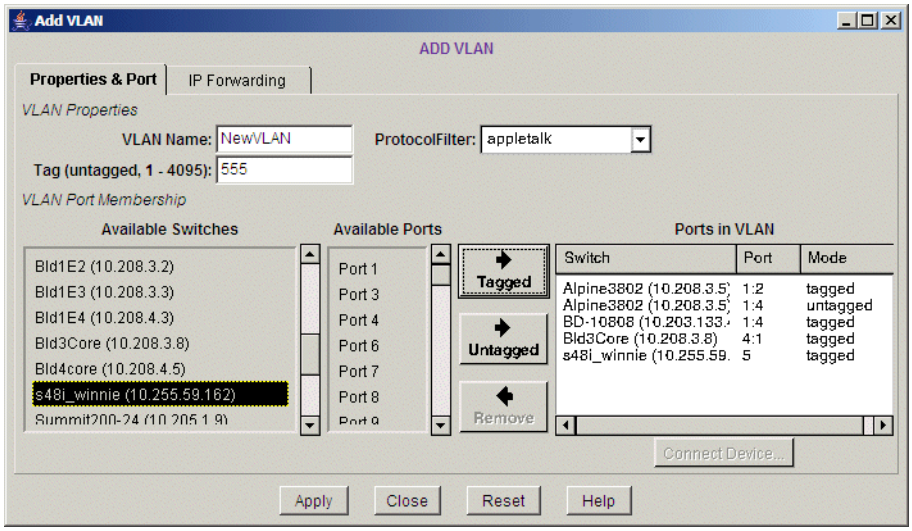
Network-wide Multidevice VLAN Configuration

Through the EPICenter VLAN Manager you can configure VLANs across multiple devices on your network in a single operation. When you create a VLAN in the VLAN Manager, you can specify ports from all the devices that should participate in the VLAN in one operation, and EPICenter will configure the VLAN on all the devices and ports you specify. You do not need to create the VLAN separately on each device.

To create a VLAN in the VLAN Manager, click the **Add** button to open the **Add VLAN** dialog.

Figure 40 shows an example of the **Add VLAN** dialog, illustrating how you can specify ports from multiple devices when you create the VLAN.

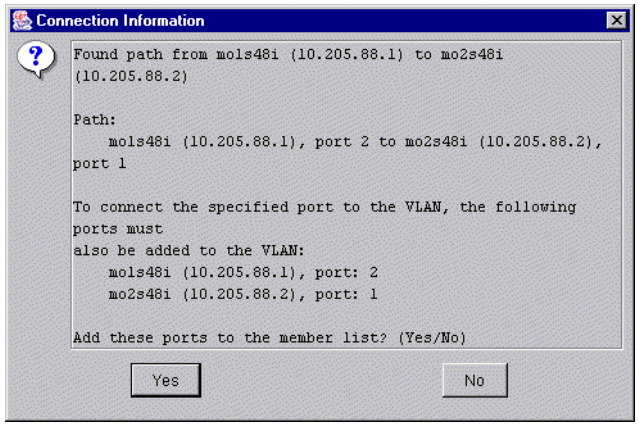
Figure 40: Creating a VLAN and defining port membership across multiple devices



Under the Properties & Ports tab of the Add VLAN dialog, EPICenter provides a list of all the switches and ports that are available to be added to the VLAN. You can select ports from each switch on which the VLAN should be configured, and add them to the Ports in VLAN list, either as tagged or untagged ports.

You can use the **Connect Device** button to have EPICenter determine whether a path exists between a device and port you have selected to add, and other devices and ports in the VLAN. The **Connect Devices** function looks for a path between a selected device and port and other members of the VLAN. If it finds a path, it displays a Connection Information window that displays information about the path. It can also determine whether additional ports, or devices and ports, need to be added to the VLAN to accomplish the needed connection. Figure 41 shows an example of this type of information.

Figure 41: Connection Information for a new port member of a VLAN


Connection Information
Found path from mols48i (10.205.88.1) to mo2s48i (10.205.88.2)
Path:
mols48i (10.205.88.1), port 2 to mo2s48i (10.205.88.2), port 1
To connect the specified port to the VLAN, the following ports must
also be added to the VLAN:
mols48i (10.205.88.1), port: 2
mo2s48i (10.205.88.2), port: 1
Add these ports to the member list? (Yes/No)
Yes
No

When you click **Apply** to create the VLAN, EPICenter will create the VLAN on all the specified devices with the specified ports. By using multi-threading EPICenter can initiate these requests concurrently on multiple devices, thus reducing the overall elapsed time required to implement those changes on the devices.

When you modify VLAN membership to delete port members or add new ports or devices and ports, again EPICenter will perform any configuration changes needed across all devices in the VLAN.

You can modify a VLAN either by clicking the **Modify** button in the VLAN Manager Toolbar, or by selecting a VLAN or device and selecting **Modify VLAN Membership** from the right-click pop-up menu. Modify VLAN Membership is available on the right-click pop-up menu from a selected device or VLAN in the By VLAN Component Tree, and from a selected VLAN (but not from a selected device) in the By Switch Component Tree.

The **Modify VLAN Membership** dialog lets you add and delete ports and devices and ports from the selected VLAN; the **Modify VLAN** dialog also lets you change other VLAN properties (such as its tag or Protocol Filter) and change the IP Forwarding behavior, if necessary.

Modifying VLANs from a Topology Map

From a Topology map, you can add ports to the VLANs in your network in two ways:

- You can select one or more links on the map, and add them to an existing VLAN. Adding a link to a VLAN will create the VLAN on the devices and ports that define the endpoints of the link(s) you select (or add the appropriate port to the VLAN if it already exists on the device). You can also create a new VLAN using the Add Links to VLAN feature.
- You can select a device on the map, and add device edge ports to an existing VLAN.

You do not need to be displaying VLAN information to perform these functions.

To add links to a VLAN:

1 Select one or more links on the map (using Shift-click to select multiple links)

2 Click **Add Links to VLAN** from the Tools menu.

This opens a dialog where you can select a VLAN to which the links should be added, or you can specify that they should be added to a new VLAN.

If you choose to add the links to an existing VLAN, you can specify whether the endpoints of the links should be added as tagged or untagged ports.

If you choose to create a new VLAN, a further dialog lets you specify the VLAN name, tag, and protocol for the VLAN, as well as whether the endpoints should be added as tagged or untagged ports.

Once you click OK, EPICenter will add the device ports that define the link endpoints to the VLAN on all the affected devices. As in the VLAN Manager, EPICenter can initiate this concurrently across multiple devices.

To add edge ports to a VLAN:

1. Select a device on the map
2. Select **Connect Edge Port to VLAN** from the Tools menu. This opens a dialog window where you can select the VLAN to which the port should be added, and select a port to be added (you can only select one port at a time to be added).

   The VLAN you select does not need to exist on the device.

   EPICenter will look for a network path that will allow it to connect the port to the VLAN you have selected. If it cannot find a path, it presents a warning, but gives you the option of creating the VLAN on the device. If you elect to proceed, EPICenter informs you of the action it will take, and gives you the option of proceeding or cancelling.

One benefit to creating or modifying VLAN port membership through a Topology map is that it makes it easy to determine whether you are adding link ports or edge ports to a VLAN, as the Topology map determines that for you. In the VLAN Manager, you need to know which ports on the device are the ones you need to add to the VLAN, depending on the role of those ports in the VLAN.

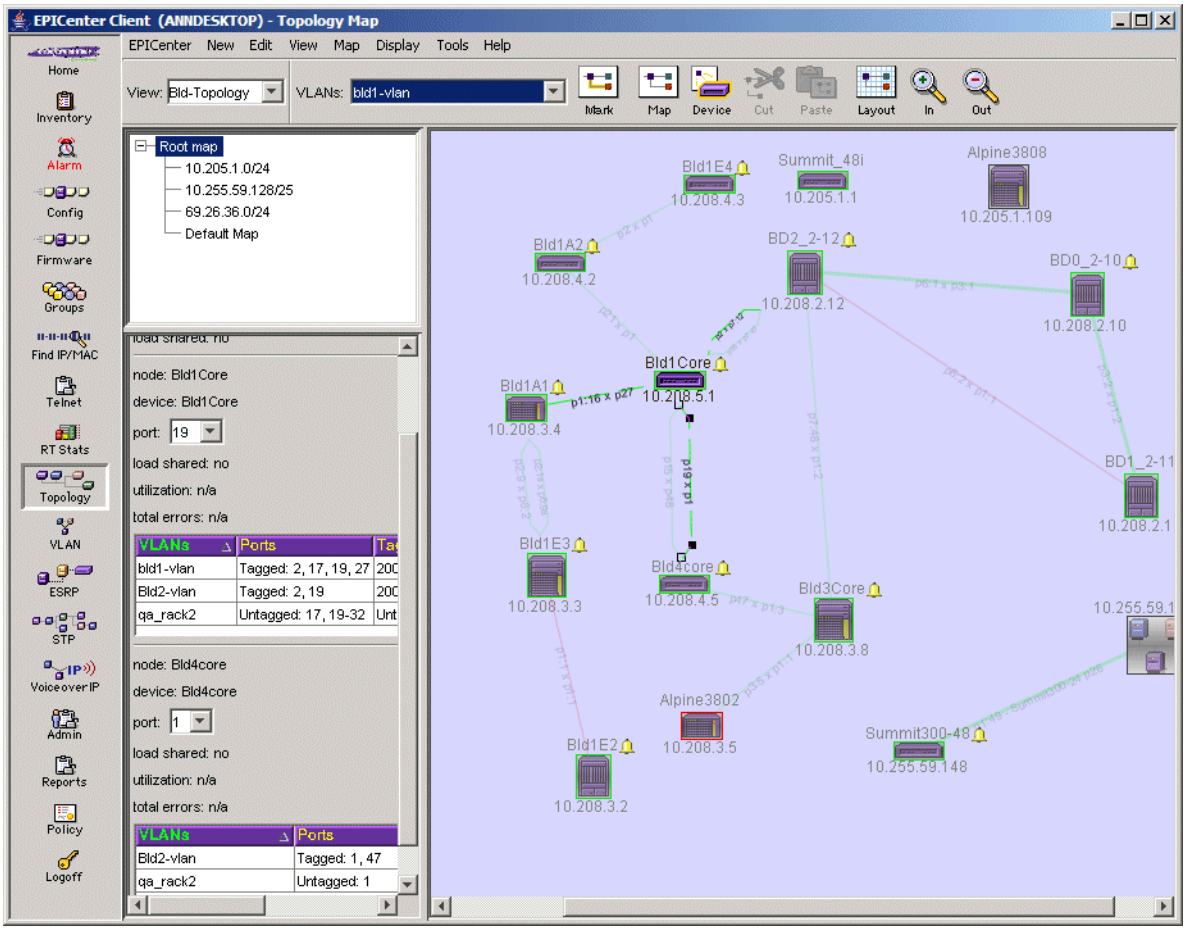
You cannot delete ports from a VLAN (or delete entire VLANs) from the Topology applet. You also cannot modify other properties of the VLANs, such as the Protocol Filters used, the VLAN tag, or the IP Forwarding behavior, from the Topology applet—those must be changed, if need be, through the VLAN Manager.

Displaying VLAN Misconfigurations with Topology Maps

Another useful aspect of viewing VLAN information through Topology maps is that is lets you visually identify misconfigured links in your VLANS. When you enable the VLAN Information view on a Topology map and select a VLAN to view, any links that are misconfigured are shown as a broken lines. A misconfigured link means that the VLAN is configured on one endpoint or the link and not the other.

The map in Figure 42 shows a misconfigured link for the displayed VLAN, *bld1-vlan*. By selecting the link and looking at the information in the Map Element Description panel, you can see that *bldg1-vlan* is configured on device Bld1Core (port 19) but is not configured on Bld4core at the other side of the link.

Figure 42: Displaying a misconfigured VLAN



You can solve the misconfiguration problem by selecting the link and using the **Add Link to VLAN** command to add the VLAN on the devices at both ends of the link. Or, if the VLAN should not be configured on either end of the link, you could use the VLAN Manager's Modify VLAN or Modify VLAN Membership commands to remove port 19 on Bld1Core from the bld1-vlan VLAN.

The ability to quickly recognize misconfigured VLAN links on a Topology map greatly simplifies the process of tracking down network communication problems among VLANs, as compared to having to inspect VLAN configuration information on a device by device basis to identify where the misconfiguration lies.

6 Managing Network Device Configurations and Updates

This chapter describes how to use EPICenter to manage your Extreme Networks device configurations. Topics include:

- Archiving device configuration files
- Creating and using Baseline configurations
- Monitoring configuration changes with baselines and the Diff function
- Managing Firmware upgrades
- Per-device change log audit of device configuration events

In a large network, the task of maintaining and backing up the configurations of your network devices, and ensuring that your devices are running the correct versions of the ExtremeWare software images, can be a difficult exercise. EPICenter's features for archiving the configuration files from your network devices, for monitoring configuration changes, and for managing the firmware versions on your devices can help you get this under control and significantly reduce the amount of administrator intervention required to keep you configurations backed up or the device firmware up to date. Further, EPICenter's ability to identify the changes to the configurations on your devices, and to maintain an audit trail of configuration updates, can help you troubleshoot when configuration problems arise.

Archiving Component Configurations

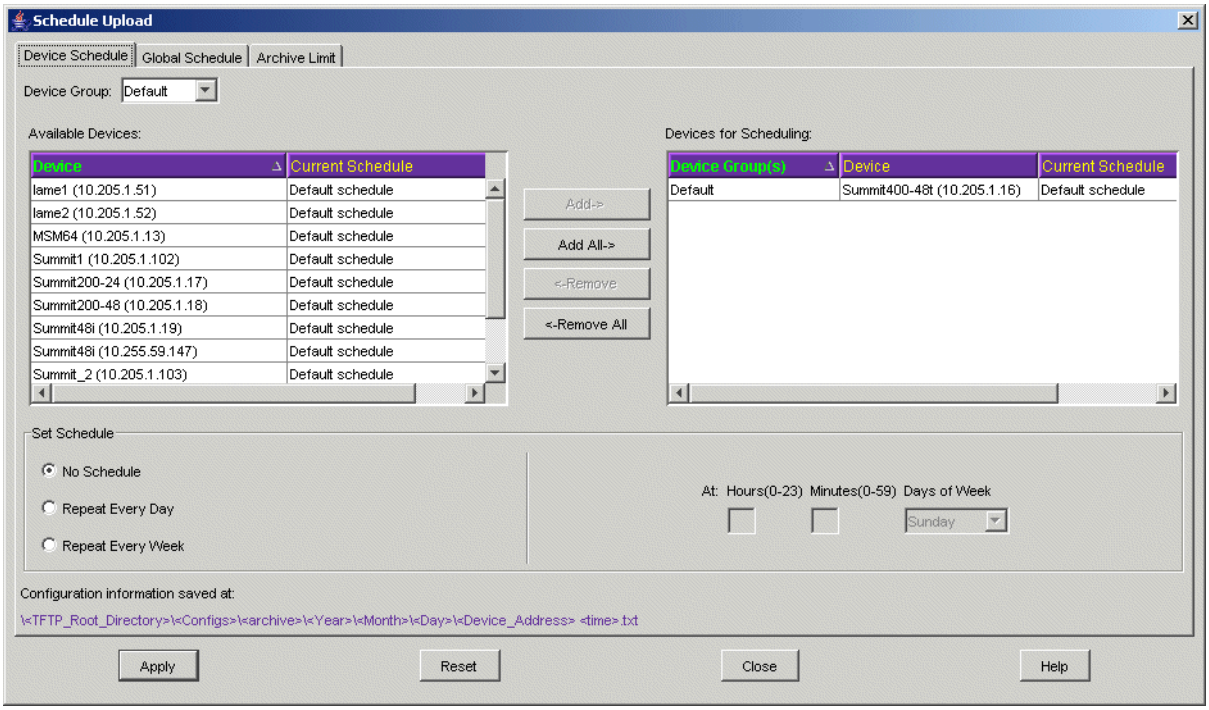
You can use EPICenter to upload and store the configuration files from all your Extreme Networks devices. You can do this on an as needed basis, but you can also have EPICenter perform archival uploads on a regular schedule without requiring administrator intervention. Thus, you can ensure that you always have back ups for your configurations in case problems arise on your devices.

To schedule regular archival uploads of the configuration files from your devices, click the Archive button in the Configuration Manager Toolbar (or select **Archive** from the **Config** menu). You can also schedule archiving for an individual device, or for the devices in a device group, by selecting the device or group in the Component Tree and then selecting **Archive** from the right-click pop-up menu.

You can create archive schedules for individual devices or for device groups, and you can create a global archive schedule for all devices that do not have individual schedules.

Figure 43 shows the Schedule Upload window for scheduling device schedules. You can select individual devices or all members of a device group for archival uploading.

Figure 43: Scheduling archival configuration file uploads



You can schedule daily or weekly uploads, and specify the time of day (and day of the week) at which they should be done. This lets you schedule uploads at times when it will have the least impact on your network load. You can create different schedules for each individual device, if that suits your needs.

Archival uploads are saved in subdirectories by the year, month and day that the archive was done. The file is named based on the device IP address and timestamp, and is in ASCII text format.

You can manage your historical archives by limiting the number of archived configurations EPICenter saves, especially if you have a large number of devices on your network or choose to do frequent archiving, You can limit either the number of files EPICenter saves for each device, or limit the length of time EPICenter keeps a file. In either case, when the limit is reached, the oldest files are deleted first.

If you don't want to schedule all your devices individually, you can set the Global Schedule, which will then archive all other devices (those not individually scheduled) based on the global schedule.

To upload configuration files from your Extreme Networks devices to EPICenter on a one-time basis, click the **Upload** button in the Configuration Manager toolbar (or select **Upload** from the Config menu). You can also initiate an upload for an individual device by selecting the device in the Component Tree and selecting **Upload** from the right-click pop-up menu. When you upload a device configuration on demand, you can save it at a location and under a filename of your choice, rather than being restricted to the default naming scheme that EPICenter uses.

Baseline Configurations

By creating baseline configuration files for your devices, you can establish a set of configurations that act as a reference configuration for the device. You can use the baseline configuration as a "known

good" configuration in case of configuration problems, and you can use it as a reference to compare against archived configuration files to identify any configuration changes that have been made.

When you view information about the configuration files that have been uploaded for a device or a device group in the main Configuration Manager window, the display indicates whether a baseline file exists for the device.

The Configuration Manager enables you to create baseline configurations in several ways:

- You can upload a configuration file from a device using the Upload feature, but specify that it should be saved as a baseline file
- You can select a saved configuration file and designate it as a baseline
- You can schedule an upload of files to be used as the baseline. This is a one-time schedule, not a repeating schedule as is done for archival uploads. This enables you to have the baseline upload performed at a time that will minimize the impact on your network load, without requiring administrator intervention.

The baseline functions are accessible from the **Config** menu of the Configuration Manager, as well as the right-click pop-up menu that is available when you have selected a device or device group in the Component Tree.

If a baseline file exists for a device, you will be able to view the baseline file using the configuration file Viewer. If both a baseline file and another configuration file exists for the device, you will be able to compare the two files using a Difference Viewer, if you have one installed on your system and have configured EPICenter to use it.

Identifying Changes in Configuration Files

If you suspect there have been changes to a device's configuration, or if you know there have been and want to identify them, you can compare two uploaded configuration files, or to compare a configuration file with the baseline file for the device. using a Difference viewer through EPICenter's **Diff** command. For example, if you suspect malicious changes, you could perform a configuration upload for the device and then compare that file with the last archived configuration.

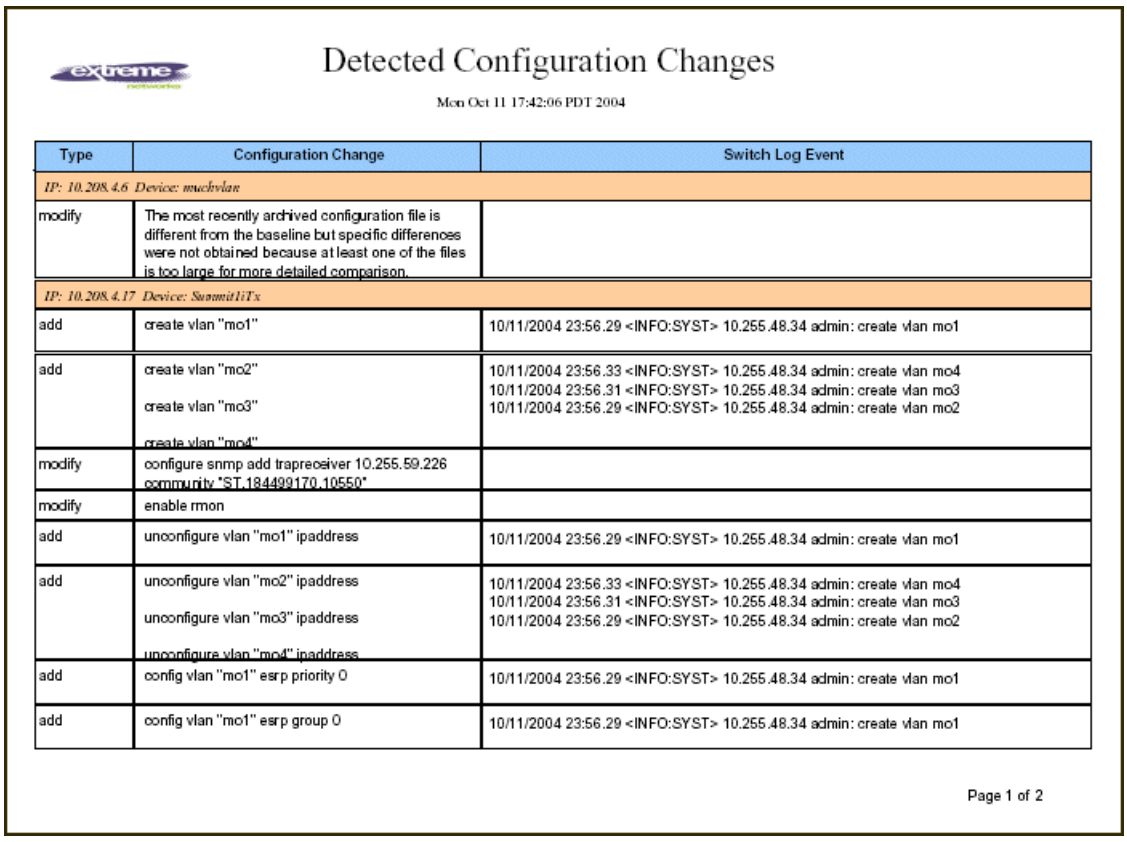
In order to use this feature you must have a Difference Viewer, such as WinMerge for Windows, or sdiff for Solaris, installed on your system. You must also specify the location of the Difference Viewer using the **Setup Viewer** command, available from the Config menu or the right-click pop-up menu under the Options submenu. You cannot view differences with a standard text editor.

Automatic Differences Detection

One of the powerful feature of EPICenter is available through the combination of baseline files and the scheduled archive feature. If a baseline file exists on the EPICenter server for a device, then when EPICenter uploads an archive configuration file for the device, it will automatically compare the new archive configuration with the baseline configuration, and create a report on those differences. In addition, if differences are detected, EPICenter will then upload the log file from the switch, and search for log entries that could explain or be related to the configuration change. EPICenter includes those log entries in the report. Based on the log entries it may be possible to identify not only when the changes were made, but also the identity of the user that made the changes.

Figure 44 shows an example of a report generated when EPICenter detects a difference between an archived configuration and the baseline configuration for a device. The report is created as a PDF file, and you can configure EPICenter to automatically email the file to recipients you designate.

Figure 44: Configuration change report for changes detected in an archived configuration



Detected Configuration Changes

Mon Oct 11 17:42:06 PDT 2004

Type	Configuration Change	Switch Log Event
IP: 10.208.4.6 Device: muchvlan		
modify	The most recently archived configuration file is different from the baseline but specific differences were not obtained because at least one of the files is too large for more detailed comparison.	
IP: 10.208.4.17 Device: SummitiiTx		
add	create vlan "mo1"	10/11/2004 23:56.29 <INFO:SYST> 10.255.48.34 admin: create vlan mo1
add	create vlan "mo2" create vlan "mo3" create vlan "mo4"	10/11/2004 23:56.33 <INFO:SYST> 10.255.48.34 admin: create vlan mo4 10/11/2004 23:56.31 <INFO:SYST> 10.255.48.34 admin: create vlan mo3 10/11/2004 23:56.29 <INFO:SYST> 10.255.48.34 admin: create vlan mo2
modify	configure snmp add trapreceiver 10.255.59.226 community "ST.184499170.10550"	
modify	enable rmon	
add	unconfigure vlan "mo1" ipaddress	10/11/2004 23:56.29 <INFO:SYST> 10.255.48.34 admin: create vlan mo1
add	unconfigure vlan "mo2" ipaddress unconfigure vlan "mo3" ipaddress unconfigure vlan "mo4" ipaddress	10/11/2004 23:56.33 <INFO:SYST> 10.255.48.34 admin: create vlan mo4 10/11/2004 23:56.31 <INFO:SYST> 10.255.48.34 admin: create vlan mo3 10/11/2004 23:56.29 <INFO:SYST> 10.255.48.34 admin: create vlan mo2
add	config vlan "mo1" esrp priority 0	10/11/2004 23:56.29 <INFO:SYST> 10.255.48.34 admin: create vlan mo1
add	config vlan "mo1" esrp group 0	10/11/2004 23:56.29 <INFO:SYST> 10.255.48.34 admin: create vlan mo1

Page 1 of 2

EPICenter will combine into one report any differences detected in archive operations that occur within a 10 hour time frame, to avoid generating many small reports. If you have a large number of devices that you are archiving, you may want to schedule them in groups with a time lapse in between that is sufficient for EPICenter to save and email a completed report.

Configuration files that are larger than 1 Mbyte cannot be analyzed with the automatic change detection feature.

Device Configuration Management Log

In the Configuration Manager, you can view the status of the most recent configuration management activity and its status—the date and time and result of the last activity (upload or download) for each device. However, there may be times when you want to view a history of the configuration management activities for a device, or for all devices.

Through the EPICenter Configuration Management Activity Report, you can view a historical log of all the configuration management activities performed through EPICenter, showing the status of the operation (whether it succeeded or failed) with additional information about the reason for the failure, if appropriate.

Managing Firmware Upgrades

Managing the versions of firmware on your devices can be a significant task, as there are a number of different versions for different device types and modules, and versions of the software and the bootROM images must be compatible as well. EPICenter can help you manage this is several ways:

- EPICenter's Firmware Manager can query the Extreme Networks web site to determine whether new versions of software are available, and can download those versions, at your option, to the EPICenter server so that you will have them available locally to use in upgrading your Extreme Networks switches.
- The Firmware Manager can compare the available software versions with the versions running in your devices and indicate whether your devices are up to date.
- The Firmware Manager can manage the upgrade process through its Upgrade Wizard, to ensure that an image or bootROM that you plan to download to a device is compatible with that device and with the bootROM on the device. The Upgrade Wizard guides you through the steps of the upgrade process, and will warn you if it detects problems.

  If multiple steps are required to accomplish the desired upgrade (i.e. you need to perform an intermediate upgrade before you can upgrade a device to the final version you want to use) the Firmware manager will inform you of the steps required and the order in which they must be performed.
- You can upgrade multiple devices in one upgrade operation, as long as all the devices in the upgrade operation are compatible with the image you are planning to download. The Firmware Manager will warn you and will not perform the upgrade if you attempt to specify devices that cannot be upgraded at the same time.

Automated Retrieval of Firmware Updates from Extreme Networks

EPICenter can connect you automatically to the Extreme Networks web site to check for new versions of software images. If it detects that new versions are available it indicates which those are, and you can select them for download from the Extreme Networks web site to your EPICenter server.

You must have a support contract with Extreme Networks in order to download software; you will need to enter your Extreme Networks support user name and password in order to login to the Extreme Networks remote server.

The Software Image Update process does not download any software to your network devices. Rather, it stores them on the EPICenter server so that you can upgrade your devices as you see necessary based on your own schedule and needs.

Detection of Firmware Obsolescence for Network Components

If you have downloaded and saved software and bootROM images on the EPICenter server, the Firmware Manager will compare the current device image against the most recent image available on the EPICenter server, and will inform you if the device is out of date. This is indicated in the device information presented when you select a device or a device group in the Component Tree in the Firmware Manager main window.

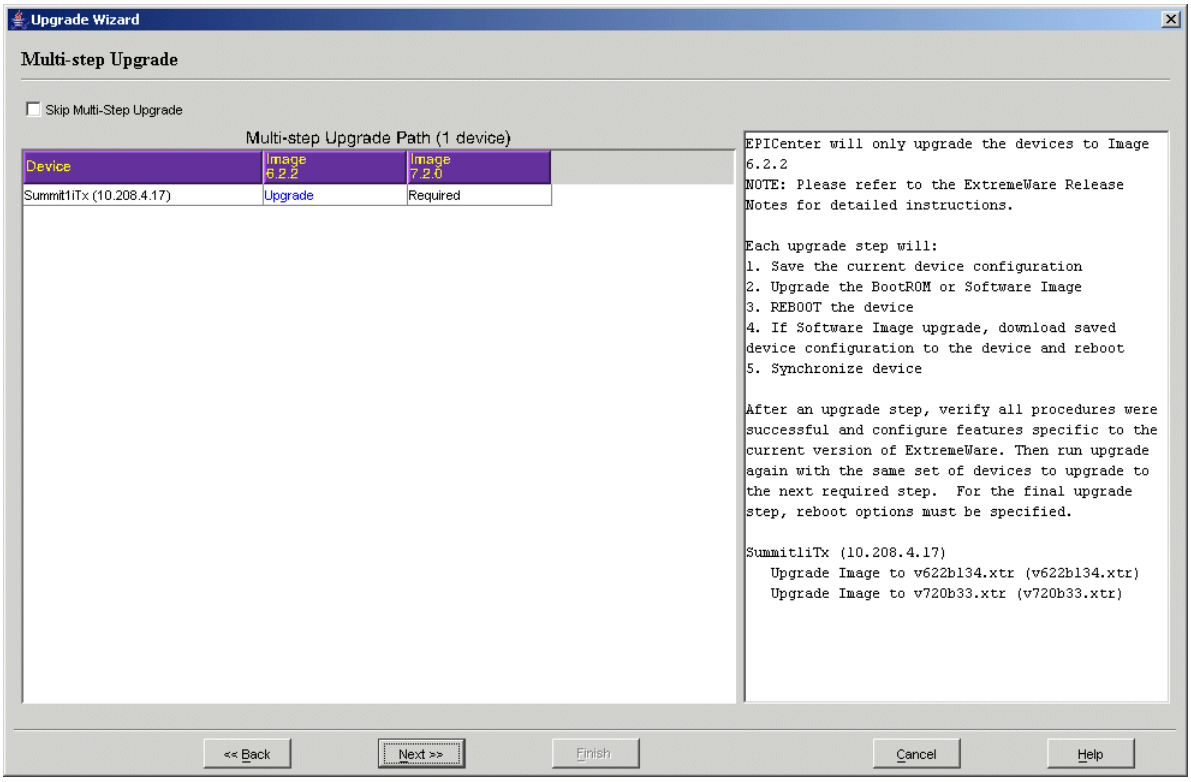
Multi-Step Upgrade Management

If you have software versions on your devices that are several revisions old, it may be that you cannot upgrade to the latest software in a single step. Upgrading may require upgrades to both the bootROM

and the software images, and you may need to do an intermediate software upgrade in order to upgrade to the most current version.

If you request an upgrade that cannot be done in one step, the Firmware Manager will determine what the required steps are, and will provide that information to you as you proceed through the upgrade process.

Figure 45: Multi-step upgrade information display


Upgrade Wizard
Multi-step Upgrade
Skip Multi-Step Upgrade
Multi-step Upgrade Path (1 device)
Device
Image 6.2.2
Image 7.2.0
Summit1iTx (10.208.4.17)
Upgrade
Required
EPICenter will only upgrade the devices to Image 6.2.2
NOTE: Please refer to the ExtremeWare Release Notes for detailed instructions.
Each upgrade step will:
1. Save the current device configuration
2. Upgrade the BootROM or Software Image
3. REBOOT the device
4. If Software Image upgrade, download saved device configuration to the device and reboot
5. Synchronize device
After an upgrade step, verify all procedures were successful and configure features specific to the current version of ExtremeWare. Then run upgrade again with the same set of devices to upgrade to the next required step. For the final upgrade step, reboot options must be specified.
Summit1iTx (10.208.4.17)
Upgrade Image to v622b134.xtr (v622b134.xtr)
Upgrade Image to v720b33.xtr (v720b33.xtr)
<< Back
Next >>
Finish
Cancel
Help

It will also proceed to do the first upgrade in the set of recommended upgrades.

When the first upgrade is finished, you can request the same upgrade again, and EPICenter will again determine whether multiple steps are needed. If so, it will set up to perform the next step in the series. This process can be repeated until the final images are installed.

NOTE

*EPICenter makes the determination of the steps required for the upgrade based on the **current** image. If the primary and secondary images do not match, then the multi-step upgrade may not do the right thing.*

7 Managing Network Security

This chapter describes how you can use the features of EPICenter to help you ensure the security of your network. It covers the following topics:

- Security Overview
- Network Access Security
- Management Access Security
- Monitoring Switch Configuration Changes
- MAC Address Finder
- Using Alarms to Monitor Potential Security Issues
- Device Syslog History

Security Overview

Network security is one of the most important aspects of any enterprise-class network. Security provides authentication and authorization for both access to the network and management access to the network devices. Network administrators must protect their networks from unauthorized external access as well as from internal access to sensitive company information. Extreme Networks products incorporate multiple security features, such as IP access control lists and virtual LANs (VLANs), to protect enterprise networks from unauthorized access.

EPICenter provides multiple features that control and monitor the security features on Extreme Networks products. Using EPICenter, you can set up VLANs, configure security policies, and monitor security aspects of your network.

Management Access Security

Along with securing the traffic on your network, you must set up your network switches to allow only authorized access to the switch configuration and traffic monitoring capabilities. This requires securing the switch to allow only authenticated, authorized access, and securing the management traffic between the switch and the administrator's host to ensure confidentiality.

Using RADIUS for User Authentication

EPICenter can function as either a RADIUS server, or as a RADIUS client.

Enabling EPICenter as a RADIUS server means that Extreme switches can act as RADIUS clients, authenticating users against the RADIUS server's database of users, as administered through EPICenter. Thus, even if a user accesses the switch directly through Telnet or a browser, the RADIUS server will provide the authentication service.

Enabling EPICenter as a RADIUS client lets EPICenter use RADIUS to authenticate users attempting to login to the EPICenter server. In addition, an external RADIUS server can be configured to return user role information as well as the user authentication.

Setting up EPICenter Roles using RADIUS

Fundamental to administrator access and control of your Extreme Networks products is setting up one or more administrator roles on each switch. A role determines what actions the administrative user is allowed on the switch or through EPICenter. For example, you need a superuser equivalent administrator who controls and monitors all products in the network. You may also want to create one or more sub-administrative roles to allow others to monitor the network without giving them the ability to reconfigure the network. To create user roles in EPICenter you add new roles using the Admin Manager and enable access to the appropriate EPICenter features.

If EPICenteris configured as a RADIUS client, when a user attempts to login to the EPICenter server, EPICenter will request authentication from an external RADIUS server. The external RADIUS server can also be configured to return role information to EPICenter as a Vendor-Specific Attribute (VSA) along with a successful authentication. You must create corresponding roles in the EPICenter Administration applet for every role that the RADIUS server may return. For example, you configure a monitor-only role in the Administration applet. You then assign the corresponding monitor-only group to the users in the RADIUS database you want to give monitoring rights to. When that user authenticates with RADIUS, the RADIUS sever returns the monitor-only group VSA which EPICenter used to assign the appropriate management role to the user.

If a user is authenticated with a role that EPICenter does not recognize, the user will be given the Monitor role by default. See "Configuring a RADIUS Server to Pass Roles" in Appendix B in the *EPICenter Reference Guide* for information on configuring a RADIUS server to pass role information to EPICenter along with the user authentication.

Securing Management Traffic

Management traffic between a management application like EPICenter and the managed network devices can reveal confidential information about your network if this traffic is transmitted in the clear. Two approaches to encrypting this traffic is managing the network products using SNMPv3, or accessing the network product directly using SSH.

Using SNMPv3 for Secure Management

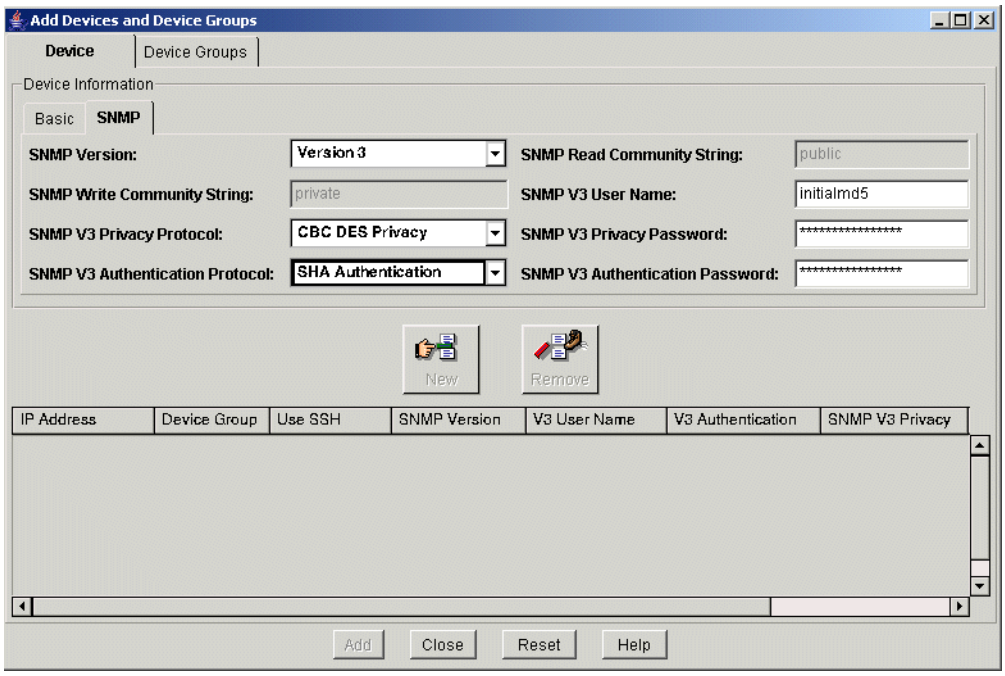
SNMPv3 is a series RFCs (RFC 2273 through RFC 2275) defined by IETF to provide management capabilities that guarantee authentication, message integrity, and confidentiality of management traffic. SNMPv3 includes the option to encrypt traffic between the agent (residing on the network device) and the management application (EPICenter). This prevents unauthorized eavesdropping on sensitive management data.

The EPICenter **Inventory Manager** can discover SNMPv3 devices in your enterprise network. Click on the **Discover** button to set the discovery options for building an inventory of your network. Select the SNMPv3 discovery checkbox to add SNMPv3-enabled devices to your inventory.

You can also add a device to the Inventory Manager, manually entering the SNMPv3 settings for the device. This includes the authentication and privacy settings for SNMPv3 and the passwords.

Figure 46 shows an example of adding an SNMPv3 device that uses CBC DES privacy and SHA authentication protocols.

Figure 46: Adding an SNMPv3 Device to Inventory Manager



The top level display for the Inventory Manager shows all the device groups configured in your network. Select a device group to determine what SNMP version is configured for each device in that group.

If you change the contact password or SNMP community string, EPICenter will ask if you want to change these settings on the device as well as in the EPICenter database. If you choose not to change the settings on the device, you will need to configure them manually on each device before EPICenter will be able to access them. If you change the SNMPv3 settings, you will also need to Telnet to the device and change those settings locally.

You could use a **Telnet Macro** in the EPICenter Telnet feature to configure SNMPv1 or SNMPv3 on a series of devices. For example, if you wanted to migrate multiple devices from SNMPv1 to SNMPv3, follow these steps:

1 Configure a **Telnet Macro** on all the devices to set up SNMPv3 and run the macro.

2 Use **Modify Device** across those same devices to change EPICenter to use SNMPv3. EPICenter allows you to modify multiple devices at the same time.

If you have both SNMPv1 and SNMPv3 on a device, EPICenter makes it very easy to switch between one and the other. This means that if you have enabled SNMPv3 on your devices, and then find it necessary to return to SNMPv1 for any reason, you can do so with minimal effort.

Using SSHv2 to Access Network Devices.

Extreme Networks products support the secure shell 2 (SSHv2) protocol to encrypt traffic between the switch management port and the network management application (EPICenter). This protects the sensitive data from being intercepted or altered by unauthorized access. You configure SSHv2 for EPICenter in the Admin feature, using the Server Properties section.

To enable SSH on a device from EPICenter, follow these steps:

1. The device must be running a version of ExtremeWare that supports SSH. This requires a special license due to export restrictions. Refer to the *ExtremeWare Software User Guide* for licensing information.
2. Install the "EPICenter SSH Enabling module". This is an SSH enabling key that can be obtained from Extreme Networks. Refer to the *EPICenter Installation and Upgrade Note* or the *EPICenter Release Notes* for information on how to obtain this key.
3. Install an SSH client on the same server as the EPICenter server. EPICenter supports PuTTy in a Windows environment, and OpenSSH in a Solaris environment.
4. Set the path to the SSH client in EPICenter, using Admin Manager. EPICenter will use this as the SSH client.
5. Enable SSH on the devices for which you want EPICenter to use SSH for direct communications.

EPICenter will now use SSH instead of regular Telnet for direct communications with the device, including Netlogin and polling for the FDB from the Extreme Networks switches.

Note that you can also use Secure Copy (SCP) and Secure FTP (SFTP) with EPICenter if you have an SSH client installed on the same system with the EPICenter server.

Monitoring Configuration Changes

Fundamental to securing your network is verifying that no configuration changes have occurred that may have a detrimental effect on network security. Something as simple as changing passwords can introduce a weakness in your security design for the network.

The EPICenter Configuration Manager provides several features you can use to monitor the integrity of your device configurations:

- You can save baseline configurations for each of your devices. Not only do these provide a known-good backup if needed, but EPICenter can then compare these to your regularly-scheduled configuration archive files to determine if any configuration changes have been made. If it detects changes, EPICenter will inspect the Syslog file for the device to identify any entries that are related to the configuration changes observed in the archived configuration file.
- Regularly archiving your device configuration files provides a backup in case a configuration is accidentally or intentionally changed.
- The Configuration Manager's **Diff** feature lets you compare two saved configuration files, or compare a saved configuration file against the baseline configuration for the device to see the differences between the two files. You must have a Differences viewer installed on the system where

you EPICenter server is installed. You can configure the Diff Viewer using the Setup Viewers command from the Options submenu of the Config menu or the right-click pop-up menu in the Configuration Manager.

See Chapter 6, “Managing Network Device Configurations and Updates” for more information on using these features of the Configuration Manager.

MAC Address Finder

You may need to track down a specific host on your enterprise network. This host may be involved in malicious activity, be a compromised source for virus infections, be using excessive bandwidth, or have network problems. EPICenter provides the IP/MAC Address Finder tool to locate any MAC address on your network.

EPICenter provides two ways to find a MAC address in your enterprise network.

If you have MAC Address Polling enabled, you can use a database search that searches the MAC FDB information learned by EPICenter's MAC Address Poller. The MAC Address Poller maintains a database on the EPICenter server of all MAC addresses associated with edge ports. An edge port is identified by the absence of Extreme Discovery Protocol (EDP) packets on a port. You can additionally disable MAC Address Polling on specific ports and switches. This is useful for disabling polling on trunk ports on third-party switches that do not use EDP.

The MAC Address Poller determines the set of MAC address on the edge ports via the FDB database on the switch. It also keeps track of the IP address(es) associated with the MAC address using the IP ARP cache on the switch. The database search is faster than the network search, although the database may be less up to date, as a full MAC address poll cycle can take a reasonably long time. However, if you want to identify the switch port where the host is connecting to the network, then a database search has the advantage of automatically ignoring trunk ports.

EPICenter also provides a full network search to search the forwarding database (FDB) and IP ARP cache on selected switches. A network search has the advantage of searching the most up to date source of data. Also, it supports searches on third party devices and on trunk ports, which transmit Extreme Discovery Protocol (EDP) packets. The network search is slower because it must contact each switch directly. It also does not always report the correct IP address associated with a MAC address / VLAN port when the MAC address is mapped to multiple IP address on the switch.

If you want to determine how a MAC address is propagating through the network aggregation layer, then a network search should be used.

Using Alarms to Monitor Potential Security Issues

The EPICenter Alarm Manager allows you to create custom alarm conditions on any supported MIB object known to EPICenter. Using the Alarm Manager, you can set up alarms for alerting you to critical security problems within your network. An example of this would be creating an alarm to notify you of a potential Denial of Service (DoS) attack.

A DoS attack occurs when a critical network or computing resource is overwhelmed so that legitimate requests for service cannot succeed. In its simplest form, a DoS attack is indistinguishable from normal heavy traffic. Extreme Network switches are not vulnerable to this simple attack because they are designed to process packets in hardware at wire speed. However, there are some operations in any

switch or router that are more costly than others, and although normal traffic is not a problem, exception traffic must be handled by the switch's CPU in software.

Some packets that the switch processes in the CPU software include:

- Learning new traffic
- Routing and control protocols including ICMP, BGP and OSPF
- Switch management traffic (switch access by Telnet, SSH, HTTP, SNMP, etc.)
- Other packets directed to the switch that must be discarded by the CPU

If any one of these functions is overwhelmed, the CPU may become too busy to service other functions and switch performance will suffer. Even with very fast CPUs, there will always be ways to overwhelm the CPU by with packets requiring costly processing.

DoS Protection is designed to help prevent this degraded performance by attempting to characterize the problem and filter out the offending traffic so that other functions can continue. When a flood of packets is received from the switch, DoS Protection will count these packets. When the packet count nears the alert threshold, packets headers are saved. If the threshold is reached, then these headers are analyzed, and a hardware access control list (ACL) is created to limit the flow of these packets to the CPU. With the ACL in place, the CPU will have the cycles to process legitimate traffic and continue other services.

Once DoS Protection is setup on the switches, you could define an Alarm for the traps "DOS Threshold cleared" and "DOS Threshold reached", and have it take an action such as an Email notification or sending a page to a network administrator.

Refer to the *ExtremeWare Software User Guide* for information on configuring DoS Protection on your Extreme Networks switches.

Another example would be to detect a TCP SYN flood as indicating a potential DoS attack. A SYN flood occurs when a malicious entity sends a flood of TCP SYN packets to a host. For each of these SYN requests, the host reserves system resources for the potential TCP connection. If many of these SYN packets are received, the victim host runs out of resources, effectively denying service to any legitimate TCP connection.

Using the Alarms Manager, you can detect a potential SYN flood by defining a threshold alarm, using a delta rising threshold rule on the TCP-MIB object tcpPassiveOpens. If this MIB object rises quickly in a short delta period, the system may be under a DoS attack.

See "Using the EPICenter Alarm System" on page 41 for more information about creating alarms such as these.

Device Syslog History

Syslog messages report important information about events in your network. Each Extreme Networks products acts as a syslog client, sending syslog messages to configured syslog servers. These messages include information that reveals the security status of your network. Using syslog messages, you can track events in your network that may affect security.

EPICenter creates a dynamic log of syslog messages in the Reports feature. Use this log to scan for critical security events such as:

Table 3: Security-based Syslog Messages

Error Message	Explanation
`<CRIT:IPHS> Possible spoofing attack`	You have a duplicate IP address on the network (same as an address on a local interface). or The IP source address equals a local interface on the router and the packet needs to go up the IP stack i.e., multicast/broadcast. In the BlackDiamond, if a multicast packet is looped back from the switch fabric, this message appears.
`USER: Login failed for user through telnet`	A login attempt failed for an administrative user attempting to connect to a device using telnet.
`SYST: card.c 1000: Card 3 (type=2) is removed.`	A card has been removed from the device. This is a possible breach of physical security if this is an unauthorized removal.
`<WARN:KERN> fdbCreatePermEntry: Duplicate entry found mac 00:40:26:75:06:c9, vlan 4095`	A duplicate MAC address appeared on the network. This is a possible client spoofing attempt.

You must make sure the EPICenter is configured as a Syslog server on the devices you want to monitor. One convenient way to do this is to use a Telnet macro—you can perform this on the multiple devices in your network in one operation. See "Example 1: A Macro to Configure EPICenter as a Syslog Server on a Device" on page 79 for an example of a script to perform this function.

Network Access Security

Network administrators need to prevent unauthorized access to their network to protect sensitive corporate data as well as to guarantee network availability. To achieve this, you need to combine edge security features such as firewalls with network controls such as IP access lists and network segmentation using VLANs. Unauthorized access attempts can originate from hosts external to your network as well as from benign or malicious attempts from within your network that can disrupt or overload your enterprise network. Using EPICenter, you can configure access lists to allow or deny traffic on your network, and you can configure VLANs to segment your physical LAN into multiple isolated LANs to separate departmental or sensitive traffic within your enterprise network.

Using VLANs

VLANs segment your physical LAN into independent logical LANs that can be used to isolate critical segments of your network or network traffic from one another. Using VLANs, you can create autonomous logical segments on your network for different business needs, such as creating a Marketing VLAN, a Finance VLAN, and a Human Resources VLAN. All the hosts for marketing personnel reside on the Marketing VLAN, will all the hosts for finance personnel reside on the Finance VLAN. This isolates marketing and finance traffic and resources, preventing any unauthorized access to financial information from any other group.

VLANs work by assigning a unique VLAN ID to each VLAN, and then assigning hosts to the appropriate VLAN. All traffic from that host is tagged with the VLAN ID, and directed through the network based on that VLAN ID. In the marketing and finance example, each department can be on the

same physical LAN, but each is tagged with a different VLAN ID. Marketing traffic going through the same physical LAN switches will not reach Finance hosts because they exist on a separate VLAN.

Extreme Networks switches can support a maximum of 4000 VLANs. VLANs on Extreme Networks switches can be created according to the following criteria:

- Physical port
- 802.1Q tag
- Protocol sensitivity using Ethernet, LLC SAP, or LLC/SNAP Ethernet protocol filters
- A combination of these criteria

For a more detailed explanation of VLANs, see the *ExtremeWare Software User Guide*.

Using the EPICenter VLAN Manager

The EPICenter VLAN Manager creates and manages VLANs for Extreme Networks devices. In the EPICenter system, a VLAN is defined uniquely by the following:

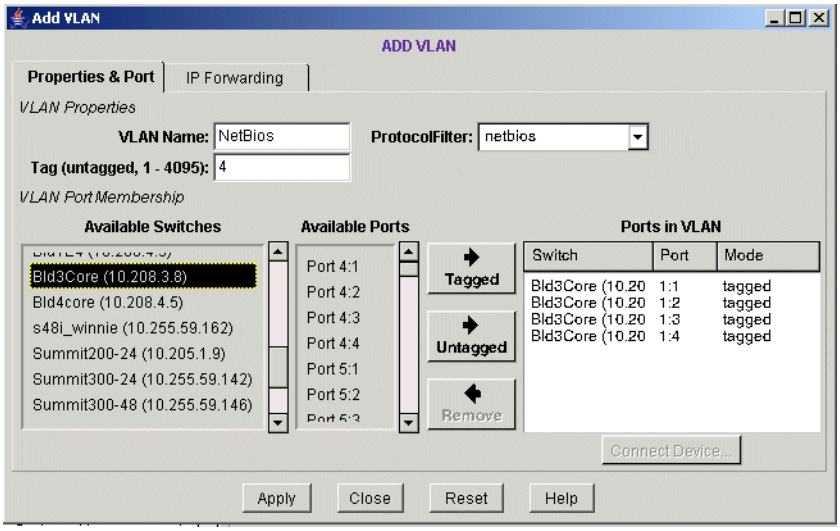
- Name
- 802.1Q tag (if defined)
- Protocol filters applied to the VLAN

As a result, multiple switches are shown as members of the same VLAN whenever all the above are the same. The VLAN Manager allows you to create VLANs from a list of available switches and ports. Based on your VLAN design, you segment your network into VLANs using the following steps:

1. Select a VLAN Name, a VLAN Tag, and protocol filter. Verify that your VLAN tag is not in use on any other VLAN.
2. Add switches and ports that match your VLAN design and mark them as tagged or untagged.
3. Verify your VLAN configuration using the view by VLAN or view by Switch option in the VLAN Manager.

Figure 47 shows a VLAN that will isolate NetBIOS traffic from the rest of your enterprise network.

Figure 47: Creating NetBIOS VLAN



See Chapter 5 “Managing VLANs” for more information about how EPICenter can help you manage the VLANs on your network.

Using IP Access Lists

IP access lists (ACLs) determine what traffic is allowed on your network. ACLs use a set of access rules you create to determine if each packet received on a switch port is allowed to pass through the switch, and if so, at what priority and with how much bandwidth, or is denied (dropped) at the ingress port. ACLs can be use to regulate both the type of traffic, the priority and minimum and maximum bandwidth (via a QoS profile), and the source or destination of the traffic allowed on your network. This is done by setting up access lists for the traffic, and determining if the traffic is allowed or denied on the network, and if allowed, what QoS Profile applies. The access list controls can be set based on the source or destination addresses. Refer to the *ExtremeWare Software User Guide* for complete description and syntax for ACLs.

You should use access lists to provide basic controls on what kind of traffic you will allow on your network. Without access lists, any traffic from anywhere can traverse your entire network. For example, you use access lists to allow HTTP traffic across your network, but deny online gaming traffic.

Designing IP Access Lists Through Policies

Access lists are configured based on policies created through EPICenter. Before creating these policies, you need to translate your security requirements into appropriate IP or security policies. To design your access list requirements, follow these steps:

1. Determine what traffic types you want to allow and deny on your network. Be sure to include both protocol types and source or destination addresses you need to allow or block. This should be based on your corporate security guidelines and the acceptable use guidelines for the hosts on your network.
2. Set your access control requirements in order of precedence. Traffic will be checked against access lists in order, using the first matching access list as the control for that traffic pattern.
3. Verify there is an appropriate “fall-through” control in your access list design. This default control is what will be used when all other access lists do not match the traffic pattern. Typically, this default control is a “deny-all” access list to block all traffic that does not match any security policy in place.

Using EPICenter to Create Access Lists

You use the optional Policy Manager feature in EPICenter to configure and monitor access lists. The Policy Manager has a set of predefined services that you can configure to control network traffic between users, devices or groups of users and devices. You create a set of policies to match the traffic controls you want in place on your network. You must also set up the order in which these policies will be applied. EPICenter uses these high-level policies to automatically create a set of access lists in each of the network devices affected by the policy. When traffic comes into your network, the Extreme Networks ingress switch port compares the traffic pattern (protocol, source and destination addresses and ports) with the set of configured access lists. The access list is traversed in order until a match occurs. If the traffic pattern matches an access list, that access list controls what happens to the traffic (allowing it to continue on the network, or denying it and dropping the packets at the ingress port).

You need to have the appropriate license to use the optional Policy Manager feature in EPICenter. Selecting the Policy Manager from the navigation bar in EPICenter displays the list of configured policies. To create a new policy for IP Access Lists, follow these steps:

1 Select the “New” button to create a new policy within the Policy Manager.

2 Define the new policy based on network resources (groups, devices), users (hosts or groups of hosts), and the predefined list of network resource services (protocols, allowed or denied).

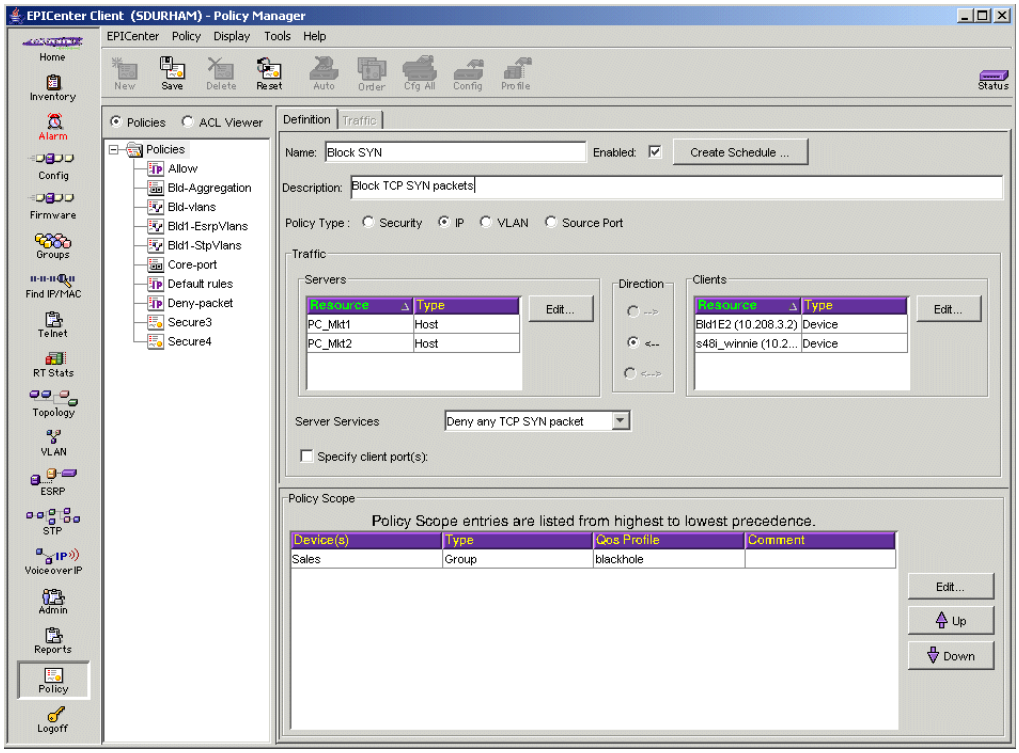
3 Save your new policy.

4 Click the “Order” button to set the order of precedence for your policies. This must match the order you determined while designing your access lists.

5 Verify your policies match your access list requirements using the ACL Viewer option in the Policy Manager.

Figure 48 shows an example of an IP based policy that will block TCP SYN packets from the network.

Figure 48: IP Policy for Denying TCP SYN Packets.



8 Managing Wireless Networks

This chapter describes:

- Wireless Networking Overview
- Inventory Management Using Wireless Reports
- Security Monitoring with Reports
- Detecting Rogue Access Points
- Detecting Clients with Weak or No Encryption
- Wireless Network Status with Reports
- Performance Visibility with Reports
- Debugging Access Issues with Syslog
- Fault Isolation with Reports
- Using Alarms to Detect Wireless Network Issues

Wireless Networking Overview

The wireless network introduces unique capabilities and management challenges to an existing wired network infrastructure. Wireless networks combine the critical network access and accountability features of a wired network with the flexibility of on-demand access and roaming. A wireless host can log into the network in one building, and then roam to another building on your corporate campus while maintaining direct access to the wired network.

Fundamental to managing wireless networks is the ability to know where your wireless clients are on the network and how they gained access to the network (authentication method, encryption, client state). You need to control not only the clients, but also any unauthorized (rogue) access points that have been connected to your enterprise network.

Wireless networks create difficult management problems that can be solved using EPICenter. With the EPICenter dynamic reports for wireless, you can monitor your wireless clients, access points (APs) and security issues unique to wireless technology.

Inventory Management Using Wireless Reports

Inventory management involves knowing what wireless network elements are connected to your enterprise networks. This includes identifying the product name, serial number, software revision and device status. The EPICenter reports feature has a pre-defined **Wireless AP Report** that lists all the wireless Extreme Networks APs attached to Extreme switches. Click on any AP in the list to get a detailed inventory report for that AP.

The **Wireless Interface Report** delves further into the configuration and status of individual interfaces associated with Wireless APs. This report details the security requirements for hosts connecting to the network through that interface as well as the number of clients associating through that interface.

Refer to Chapter 16 in the *EPICenter Reference Guide* for details on the **Wireless AP Report** and the **Wireless Interface Report**.

Security Monitoring with Reports

Wireless networks require stringent security controls to ensure identity and confidentiality within and external to your enterprise network. Without a proper security policy in place, any rogue client could gain access to your enterprise networks not only from within your physical building, but from any place within range of your APs. Because wireless extends your wired infrastructure beyond the physical limitations of cabling, your network becomes vulnerable to external security breaches if you do not control and monitor the security aspect of your wireless network. Security breaches include both unauthorized host access and unauthorized (rogue) APs that allow insecure communications beyond the boundaries of your security policy.

Client MAC spoofing report

When the network detects two or more client stations with the same MAC address that are all in the data forwarding state on different wireless interfaces, the client might be using another client's MAC address in an unauthorized way; such a client is known as a spoofing wireless client. The **Spoofing Wireless Client Report** displays information on these clients.

However, a client can also appear on two or more wireless interfaces at the same time because it is roaming and thus changing from one interface to another. To exclude these cases from the report, you can specify a wireless client time-out length (minimum connection time) to correspond to the client age-out setting on the switch.

Figure 49 shows an example of a **Spoofing Wireless Client Report** where the clients are roaming.

Figure 49: Spoofing Wireless Client Report.

sdurham
Close Window
Main
Network Summary
+ Devices
+ Slots and Ports
+ VLAN
+ Logs
- Wireless Reports
Wireless Summary
Wireless AP
Wireless Interface
Safe AP MAC List
Rogue APs
Rogue AP Alarms
Network Login
Current Clients
Client History
Spoofed Clients
Unconnected Clients
+ Client Reports
+ MIB Poller Tools
+ EPICenter Server
+ Miscellaneous
Spoofing Wireless Client Report
Report generated on October 18, 2004 07:29:02 PM
Wireless client time out length (seconds) 900 Submit
Download report in csv or xml format, or show all in one page.
Client MAC | User Name | Authentication Method | Encryption Method | Device | Interface | WP Location
00:06:25:0c:a2:45 | wliP | Net Login | None | Summit300-24 (10.255.59.142) | 1:23:1:1 | qa-cube
00:06:25:0c:a2:45 | wliP | Net Login | None | Summit300-48 (10.255.59.146) | 1:12:1:1 | test

Monitoring Unauthenticated Clients

While clients that are not yet authenticated on your network may be a normal occurrence, you may want to monitor these clients to determine if an unauthorized client is attempting to connect to your wireless network. The **Current Clients Report** lists all wireless clients known to EPICenter. This includes clients that have not yet logged in. Click on the Client State column heading to sort the client list by client state. You can determine which clients are in an unauthenticated state.

Detecting Rogue Access Points

Rogue access points (APs) occur when someone other than your network administrator connects an AP to your enterprise network. Because APs are inexpensive and simple devices, this is not an uncommon occurrence in an enterprise network. These rogue APs are a security breach that may open your network to intruders anywhere within range of the rogue AP. You must detect and remove these rogue APs to ensure a secure enterprise network.

Rogue AP detection works by detecting other APs broadcasting on the in-service channel. APs that are not known (managed) Extreme APs or already in the Safe AP list, then the AP is listed as a rogue. Rogue AP detection can also scan periodically on the out-of-service channels if that capability is enabled in the Extreme switch. Refer to the Extreme Networks software guide appropriate for your switch for configuring this capability. You can add non-Extreme APs to the Safe AP list to keep them from being marked as Rogue APs.

APs are marked as rogues in Extreme Networks switches by detecting when a new AP shows up on the network that does not appear in the list of authorized APs. The **Rogue AP Report** in EPICenter lists these unauthorized APs and gives details on the AP model, operating characteristics, and the interface that detected the rogue AP.

Enabling Rogue Access Point Detection

You must configure EPICenter to enable rogue AP detection. To do this, you configure authorized APs using the **Safe AP MAC Address List**. The Safe AP Mac List shows the list of MAC addresses that belong to Access Points that have been determined to be legitimate and added to this list. If you are an Administrator (with the Administrator role) you can also manage the list of safe MAC addresses through this page, by importing lists of MAC addresses or deleting the list. You can add individual MAC addresses to this list either through importing a list of safe MAC addresses, or by adding individual MAC addresses to the safe list.

Import Safe MAC Address List

To import a safe MAC address list, you must have write access privileges to EPICenter and follow these steps:

1. Click on the **Reports** button in the EPICenter Navigation bar and select the **Safe AP MAC List**.
2. Use the **Browse** button to browse your local system for the safe MAC address list you want to import.

   The input list is simply a text file with MAC address and optional description, separated by a comma, with one MAC address per line.
3. Click **Submit** to upload the selected safe MAC address list.

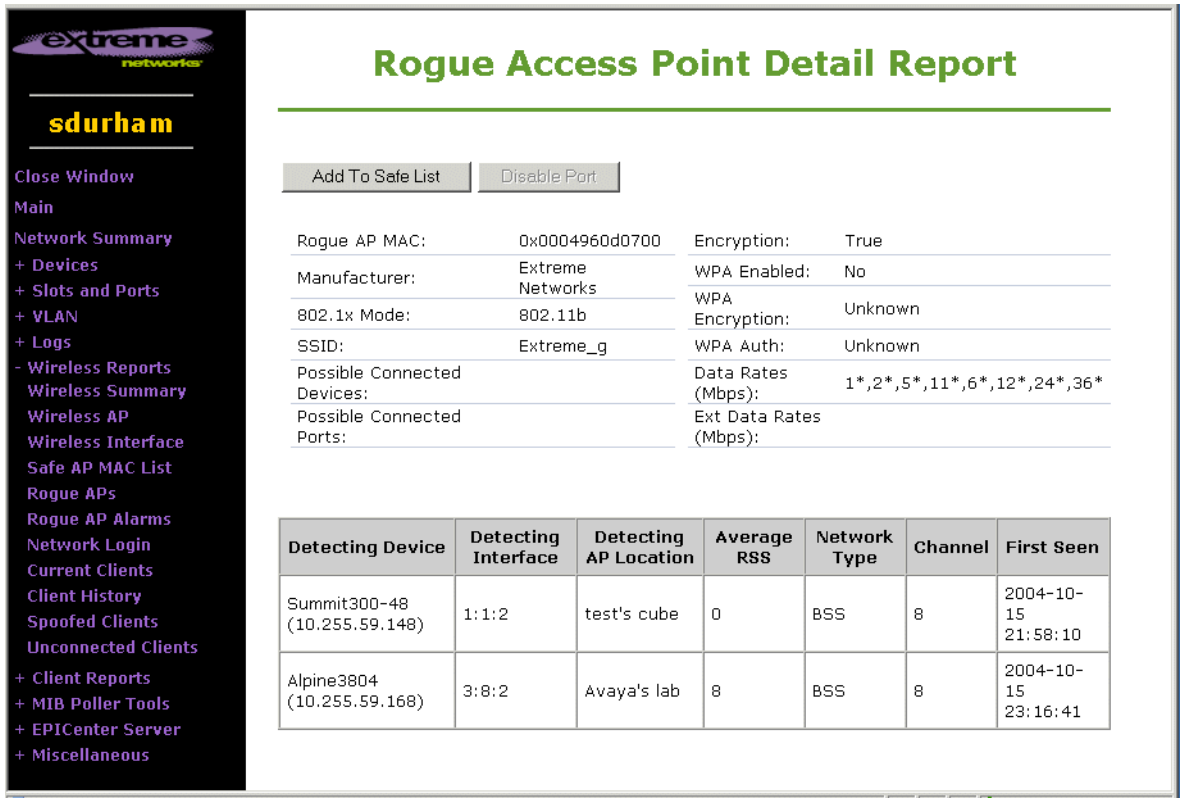
Adding Individual Devices to the Safe List

To add any AP that appears in the **Wireless Rogue AP Repor**t into the Safe AP MAC Address List, follow these steps:

1. Click on the Rogue AP MAC address in the **Wireless Rogue AP Report** that you want to add to the safe AP MAC address list. This opens the **Rogue Access Point Detail Report**.
2. Verify that this is a properly configured AP that you want to add to your safe list.
3. Click on the **Add to Safe List** button to add this AP MAC address to the EPICenter Safe AP MAC Address List. This AP will no longer show up as a rogue AP.

Figure shows an example of the **Rogue Access Point Detail Report**. Note the **Add to Safe List** button near the top left corner. Use this button to add this AP to your Safe List

Figure 50: Rogue AP Detail Report Example



Detecting Clients with Weak or No Encryption

Securing your wireless traffic is crucial to providing the flexibility of mobile, on-demand access to your enterprise network. Using wireless technology, your network traffic is no longer protected by the physical boundaries of your wired network. To prevent eavesdropping and interception of your critical data, you must monitor and control the clients accessing your wireless networks.

EPICenter provides the tools to determine the security abilities of the clients accessing your wireless network. Use the **Current Clients Report** to detect clients with weak or no encryption. This report can be sorted to show client encryption in order or you can filter the report to show no encryption or weak encryption like WEP64. To filter the report for encryption settings, follow these steps:

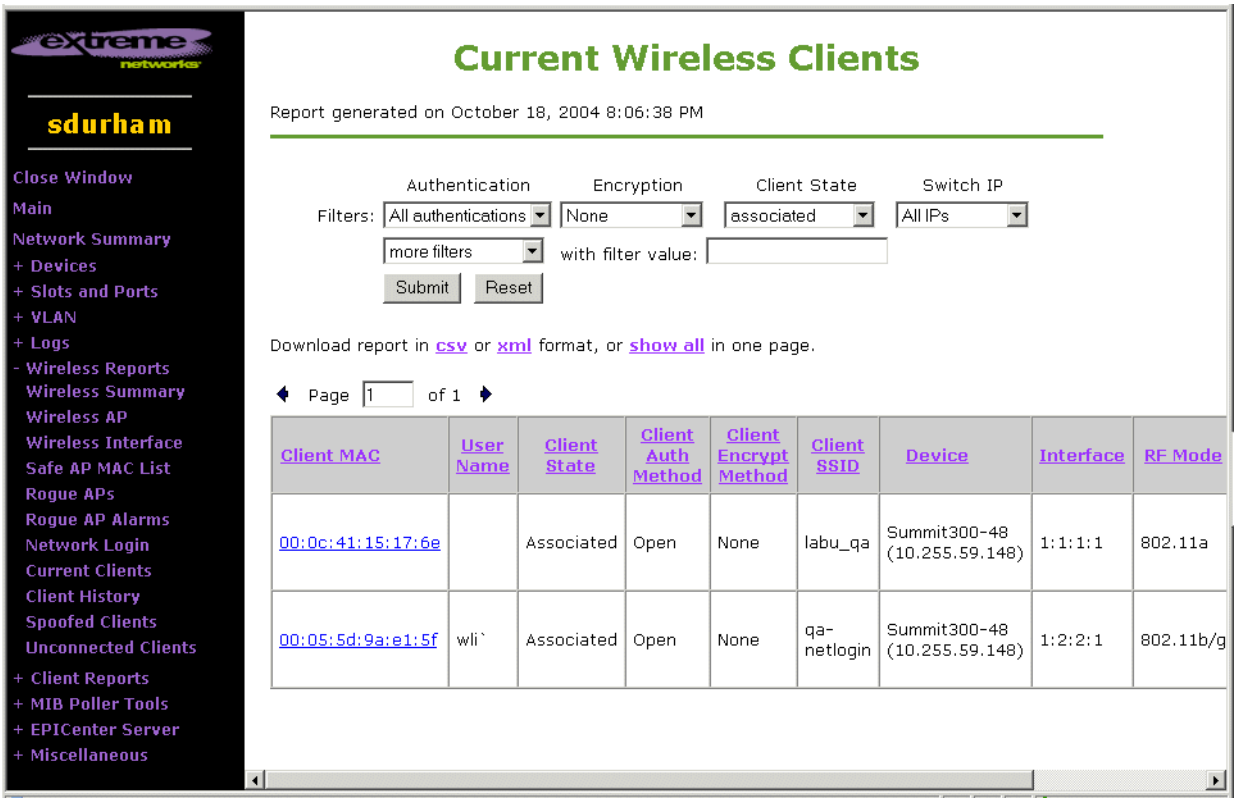
1 Click the **Reports** button in the EPICenter navigation bar to open the Reports browser.

2 Select the **Current Clients Report.**

3 Set the Encryption filter to None or WEP64 and press the **Submit** button.

Figure shows an example of a Current Clients Report filtered for clients with no encryption enabled.

Figure 51: Current Wireless Clients Report Example



Wireless Network Status with Reports

The EPICenter Reports feature provides multiple dynamic reports that can be used to monitor the status of your wireless network. These reports give a summary of the wireless network, as well as drill down details on access points, interfaces, network logins and clients.

The Wireless Summary Report shows the number of wireless ports and clients. This report also provides summaries on the number of rogue access points, unauthenticated clients, and the number of clients using different authentications methods. Each summary type provides a direct link to a detailed report on these topics.

Performance Visibility with Reports

You can use the MIB Poller feature of EPICenter to gather performance statistics on your wireless network. These SNMP statistics provide performance information on clients and access points.

To get the wireless interface client statistics and AP performance statistics, follow these steps:

1 Configure the MIB Poller using a collections.xml file, as described in “Using the MIB Poller Tools” on page 123.

2 Add the necessary MIB variables to collections.xml to match the statistics you want to monitor on your wireless interfaces.

Or, use the MIB Query tool to have EPICenter query the SNMP MIB variables for a one-shot update on the relevant statistics. Note that SNMP MIB objects with Counter or Counter64 syntax require you to compare the difference between two consecutive polls of the MIB object to collect relevant information on that statistic.

Use the extremeWirelessClientDiagTable for client diagnostics.

Use the following tables for AP performance:

- extremeWirelessIntfFrameSizeTable
- extremeWirelessIntfFrameSizeErrorTable
- extremeWirelessIntfFrameSpeedTable
- extremeWirelessIntfFrameSpeedErrorTable.

Debugging Access Issues with Syslog Reports

Syslog messages provide timely information on how your network is operating. These messages are available in the Syslog Report. Using this report, yo u can filter for syslog messages that relate to network access issues. Some syslog messages that relate to network access include:

- `USER: Login failed for user through telnet (149.127.139.142)`—This message indicates a user could not log in using telnet.
- `<INFO:SYST> User pjorgensen logged out from telnet (209.75.2.1)`–These messages indicate that a telnet connection was opened to a switch and then closed without entering the user name. The switch does not generate any entry for logging into the switch; it only generates a log message stating that a particular user has just logged out.

You must make sure the EPICenter is configured as a Syslog server on the devices you want to monitor. One convenient way to do this is to use a Telnet macro—you can perform this on the multiple devices in your network in one operation. See “Example 1: A Macro to Configure EPICenter as a Syslog Server on a Device” on page 79 for an example of a script to perform this function.

Fault Isolation with Reports

The EPICenter **Reports** feature provides dynamic reports that can be used to isolate faults in the wireless network. Using the **Unconnected Clients Report,** you can track which clients are not able to connect to the network and gather information to determine if this is caused by a common interface or access point. You can use the **Wireless Summary Report** to verify if the number of wireless ports not online is the expected level or if some of your ports have gone offline for unknown reasons.

9 Tuning and Debugging EPICenter

This chapter describes how to tune EPICenter performance and features to more effectively manage your network. It also describes some advanced features that are available to an EPICenter administrator (a user with an Administrator role) to help analyze EPICenter or Extreme Networks device operation. These include:

- Monitoring and tuning EPICenter performance
- Tuning the alarm system
- Using Device Groups to facilitate workflow
- Using the EPICenter MIB Poller tools to maintain MIB variable history
- Reconfiguring EPICenter ports
- Using the EPICenter debugging tools

Monitoring and Tuning EPICenter Performance

If you are using EPICenter to manage a very large number of devices in a large network, you may can encounter times when the performance of the system can seem slow. There are a large number of factors that can affect the performance of EPICenter. Some of these you can affect with various settings in EPICenter. In other cases, you may be able to affect the overall performance of the system by considering how you manage specific devices in your network.

There are a number of factors that can affect EPICenter performance:

- The amount of alarm processing the system is attempting to handle. This is discussed in some detail in the section "Tuning the Alarm System" on page 120.
- The frequency and timeouts for SNMP polling and MAC polling (if you have it enabled)
- The processor power and amount of memory available on the system running the EPICenter server.
- The size of the worker thread and the maximum number of SNMP sessions that can be running.

Taking a Device Offline

If a device is scheduled to be taken down for maintenance, you can set that device offline in the EPICenter database. EPICenter will not attempt to poll or sync with the device and will ignore all traps from the device while it is offline. This means that any events caused by the maintenance activities will not cause alarms in EPICenter.

- To take a device offline in EPICenter, go to the Inventory Manager, select the device in the Component Tree, and select **Take Offline** from the Inventory menu or from the right-click pop-up menu for the device. Note that this does not physically change the device; it just sets EPICenter to ignore the device as if it were offline.
- To return the device to online status when the device is again reachable, use the **Bring Online** command (which replaces the **Take Offline** command in the Inventory Menu and pop-up menu for a device that is offline).

For devices that simply take a long time to sync or to poll on a Detail poll cycle, you can reduce the impact by reducing the Detail Poll frequency (lengthening the time between polls) for those devices. The default Detail polling frequency is 30 minutes for core devices and 90 minutes for edge devices.

Polling Types and Frequencies

Upon client startup, before you can log in, EPICenter by default attempts to sync all the devices it is managing, to bring its database up to date. For devices that are down (and not marked offline in EPICenter) EPICenter will attempt to sync the device and will have to wait until the device times out. Further, a sync does a Detail Poll, so a large network with many devices with very complex configurations (for example, a large number of VLANs) the sync operation can take a fair amount of time. However, once this sync has completed, EPICenter does

EPICenter does several types of polling, using SNMP or Telnet, for the information it needs.

SNMP Polling

EPICenter does two types of polls for device information using SNMP.

- A global “heartbeat” poll that gets basic information about device reachability. The poll frequency for this is 5 minutes, for all devices regardless of type.
- A device-specific Detail poll, that polls for more detailed information about the device configuration, such as software version, bootROM version, VLANs configured on the device, and so on. This poll can take much longer to complete, so this type of polling is done less frequently, and is configurable on each device individually in the Inventory Manager. The defaults poll interval for this type of polling is every 30 minutes for core (chassis) devices and every 90 minutes for edge devices.

The global poll frequency can be changed through the Admin applet, under the **SNMP Server Properties**. Any changes will affect all devices in the EPICenter database. You can also change the timeout and number of retries.

Increasing the global SNMP polling interval can reduce the load on your server and your network, at the expense of the timeliness of device state information.

The Detail Device Poll interval can be changed in the Inventory Manager, in the Basic tab of the Modify Devices dialog (or in the Add Devices dialog). Changes here will affect only the devices selected for modification.

MAC Address Polling

EPICenter provides an option for doing Telnet-based polling of switch FDBs to gather MAC address information about edge ports. This feature is disabled by default. If enabled, its frequency can be modified to reduce the load on the overall system and the network.

MAC address polling is enabled or disabled globally through the MAC Polling Server Properties in the Admin applet. If enabled, MAC address polling can then be enabled on a per device basis through the Inventory Manager.

Through the MAC Polling Server Properties, you set the amount of load, which determines the amount of elapsed time between sets of FDB polling requests. A complete MAC address polling cycle consists of multiple groups of requests, until all devices with MAC address polling enabled have been polled.

A setting of Light (recommended) means the elapsed time between groups of MAC address polling requests will be calculated to place a lighter load on the EPICenter server. As a result, it will take longer for the server to accomplish a complete polling cycle. Moving the load indicator towards Heavy will shorten the elapsed time between groups of MAC address polling requests, at the cost of a heavier load on the EPICenter server.

You can use the EPICenter Server State Summary Report to see the MAC address polling frequency based on the current setting of the MAC Polling server properties. The Server State Summary report tells you how long it took to complete the most recent polling cycle, as well as the average time it has taken to perform a complete polling cycle. Based on this data you can determine if you need to adjust the MAC Polling System Load factor.

Telnet Polling

Telnet polling is used for MAC address polling, for retrieving Netlogin information, for retrieving ESRP information on older Extreme switches, and for retrieving Alpine power supply IDs. You cannot modify its frequency other than as discussed for MAC polling in the previous section. You can disable Telnet polling entirely, however, in the Devices area of Server Properties in the Admin applet.

If you disable Telnet Polling, MAC address polling is also disabled.

Performance of the EPICenter Server

Performance of the EPICenter server itself is affected by the number of devices you are managing as well as the resources of the system on which the EPICenter server is running.

You can use the Windows Task Manager or a tool such as `top` in Solaris (available as downloadable Freeware) to determine how much memory and processor the EPICenter server is consuming. The larger the set of devices EPICenter tries to manage, the more resources it will require. If you also run the EPICenter client on the same system as the EPICenter server, that will increase the load. You should ensure that you have adequate processing power and enough memory to allow EPICenter to run without extensive swapping.

The *EPICenter Release Note* provides information on the system requirements for the EPICenter server.

If EPICenter server performance is slow, you can look at the Thread Pool Statistics using the EPICenter Server State Summary Report. Specifically, if the Percentage Wait per Request statistic is high (greater than 20%) you can consider increasing the maximum thread pool size and the maximum number of SNMP Sessions.

To do this, go the Admin applet, and select **Scalability** under the Server Properties tab. Then increase *both* the Thread Pool Size *and* the Maximum number of SNMP sessions by between 25% to 50%

Tuning the Alarm System

Alarm activity (processing traps and executing alarm actions) can consume a fairly significant amount of system resources if you have a large number of devices in your network, with many alarms enabled and scoped on all devices. Therefore, tuning the alarm system can have a significant impact on the overall performance of the EPICenter server.

The steps you can take to help tune your EPICenter server's alarm system involve the following types of actions:

- Disabling alarms you don't care about
- Scoping alarms so they only function on for devices you care about
- Identifying individual devices that generate a lot of alarm activity, and either correcting the situation that may be producing these alarms, or removing the device from the scope of alarms that aren't necessary for the device.

Disabling Unnecessary Alarms

There are several situations where you may want to disable alarms that are unnecessary and are consuming system resources.

One immediate place to look is at the alarms that are predefined within EPICenter. The following set of alarms are predefined in the EPICenter database, and all are enabled by default, scoped for all devices and ports:

- Authentication failure (SNMP MIB-2 trap)
- Config Upload Failed (EPICenter event, indicates failure in an upload initiated by EPICenter)
- Device reboot (EPICenter event)
- Device Warning from EPICenter (EPICenter event)
- ESRP State Changed (Extreme proprietary trap)
- Fan failure (EPICenter event)
- Health Check Failed (Extreme proprietary trap)
- Invalid login (Extreme proprietary trap)
- Overheat (EPICenter event)
- Power Supply Failed (EPICenter event)
- Rogue Access Point Found (EPICenter event)
- Redundant Power Supply (RPS) alarm condition (Extreme proprietary trap)
- SNMP unreachable (EPICenter event)

If there are any of these alarms that you know are not of interest, you can disable the alarm as a whole through the Alarm Log Browser. For example, if you are not concerned about SNMP security you can disable the Authentication Failure alarm. If your network connectivity tends to be problematic or you have very slow devices, you may want to disable the SNMP unreachable alarm.

To disable an alarm you must modify its alarm definition:

1. Go to the Alarm Definition tab in the Alarm System, and select the alarm you want to disable
2. Click the **Modify** button in the upper Toolbar to open the Alarm Modify Definition window with the selected alarm definition displayed.

3 Uncheck the **Enabled** checkbox to disable the alarm, then click **OK**.

Note that disabling alarms that are not likely to occur will not have much performance impact. For example, if you do not use ESRP, the disabling the ESRP State Change alarm is not likely to have an impact, as those alarms should never occur. However, if you do use ESRP but do not want to know about state changes, disabling that alarm could have some performance impact.

One way to determine which alarms could be disabled for maximum performance impact is to look at the alarms that actually do occur within your network. You can use the Alarm Log Browser to show you which alarms occur in your network:

1 In the Alarm Log Browser, filter the alarm list to show all alarms. You can filter the log using `"Log ID > 0"` as the filter criterion to show all alarm log entries.

2 Sort the alarm list by the Name column. This groups all occurrences of a given alarm together. Using this list you can see both which alarms occur in your network, and the volume of alarms generated for each type of event.

3 If this list shows large number of alarm instances for an alarm that you don't care about, disabling that alarm could potentially have a beneficial impact on EPICenter system performance.

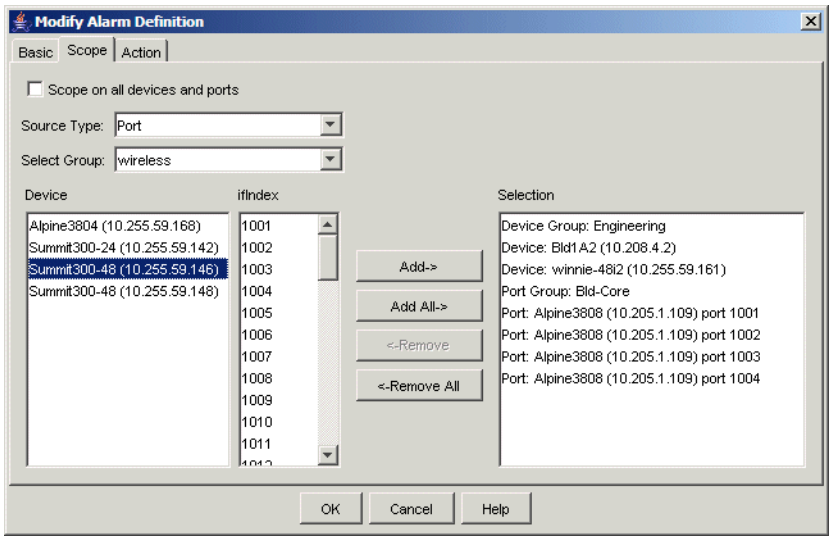
Another possibility is that a specific device is generating a large number of alarms. If this is the case, you may be able to eliminate some of this load by either reconfiguring, maintaining or repairing the device to eliminate the fault, or by changing the scope of one or more alarms to remove the problematic device from the alarm scope. By removing a device from the alarm scope, EPICenter will ignore traps for the device, and will not trigger an alarm even though the device itself may still generate those trap events.

Limiting the Scope of Alarms

One way to potentially reduce the load created by alarm processing is to use the Alarm scope to limit an Alarm to only selected devices. For example, you may want to create link down and link up alarms to monitor the status of certain critical links in your network, but ignore such events on non-critical links.

When you create an alarm, the default scope is to all devices and all ports. The **Scope** tab of the Add Alarm Definition or Modify Alarm Definition dialogs lets you specify a scope for the alarm (Figure 52).

Figure 52: Defining the scope of an alarm



You can scope an alarm to Device Groups and Port Groups as well as individual devices and ports.

To change the alarm scope for an existing alarm:

1 Under the Alarm Definition tab in the Alarm System feature, select the alarm you want to scope, and click **Modify**.

2 Select the **Scope** tab

3 Uncheck the **Scope on all devices and ports** checkbox. This enables the **Source Type** and **Select Group** fields.

4 The Source Types you can select are Device, Device Group, Port, and Port Group.

If you select either Device Group or Port Group, the area below (labeled Devices in the example) will display a list of all the Device Groups or Port Groups defined in EPICenter. When you select one or more of these, it puts the group(s) as a whole into the Selection list at the right.

If you select Device or Port, then the Select Group field lets you select a Device Group to display the devices in the group in the field below.

- If the Source Type is Devices, individual devices in the selected Device Group can be added to the selection list
- If the Source Type is Ports, individual port ifindex values can be added to the selection list.

Using Device Groups and Port Groups for Alarm Scopes

Special-purpose Device Groups and Port Groups are very useful for purposes of alarm scoping. Devices Groups are created in the Inventory Manager; Port Groups are created in the Grouping Manager. Since EPICenter allows you to put the same devices or ports into multiple different groups, you can create special purpose groups that simplify the configuration of alarm scopes.

For example, you might create a port group for the critical links on your core devices, another for edge port links or for wireless interfaces.

A major benefit of using Device and Port Groups for alarm scoping, rather than configuring the scope with individual devices and ports, is that you can then change the scope of an alarm by simply

changing the membership of the relevant groups. You can add or remove links from a Port Group, or add or remove devices from a Device Group, and the scope of the alarm will automatically reflect the changed group membership. You do not need to modify the alarm definition every time you add or change devices or ports on your network.

The Alarm and Event Log Archives

The EPICenter server stores a maximum of 50,000 events in the event log, and a maximum of 12,000 alarms in the alarm log. Both are stored as tables in the server database. Excess data from the event log and alarm log are archived to files when the logs reach 115% of their maximum size.

The event log archive is made up of two 30MB rotating archive files and includes all traps and Syslog messages. The event log is stored in a file called `event_log.txt` and the archive file is called `event_log.old`.

The alarm log archive is made up of two 6 MB rotating files and includes all alarms associated with traps and Syslog messages. The alarm log is stored in a file called `alarm_log.txt` and the archive file is called `alarm_log.old`.

An archiving check is performed once an hour. If you need to store additional historical data beyond the two 30 MB file limit for events and the 6 MB file limit for alarms, you can periodically make backup copies of the archive files to a separate location. Refer to Appendix C, “EPICenter Backup” in the *EPICenter Reference Guide* for more information about alarm log backups.

Using the MIB Poller Tools

The MIB Poller Tools, found in the Reports module, can be used to collect and inspect data from any MIB variables supported by the devices on your network. These tools allow you to retrieve data that is not available through EPICenter’s reports or other status displays, and to accumulate historical data for MIB variables of interest. The collected data can then be exported as a comma-separated text file which can be imported into another application such as a spreadsheet for analysis.

You must have an Administrator role to set up and initiate MIB collection or query actions, However, users with other roles can view the results of a collection that has been initiated by an Administrator.

There are two separate tool available for retrieving MIB variable data:

- The MIB Poller Summary displays a MIB collection, or allows an Administrator to load a MIB collection XML file to initiate MIB collection activity. A MIB collection is a historical log of MIB values as defined in the collections.`xml` file. In a running collection, EPICenter polls specified devices, retrieves the values of specified MIB variables and saves them in the EPICenter database. The OIDs and devices to be polled, the poll interval, number of polling cycles and the amount of polled data to be stored is all defined in the Administrator-created `collections.xml` file.
- The MIB Query tool allows an Administrator to create a one-time MIB query request to retrieve the value of specific variables from a set of specified devices. This is a one-shot query, and does not poll repeatedly or store the data it retrieves.

  The MIB Query tool is accessible only to users who have an Administrator role.

Defining a MIB Collection

A MIB Collection is defined in an XML file named `collections.xml` that is stored in the EPICenter `user/collections` directory of the EPICenter installation. You can specify both scalar and tabular OIDs. You must also specify the set of devices (by IP address) that should be polled for this data, and provide some additional properties such as the polling interval.

The `collections.xml` file must have the following format:

```
<?xml version="1.0" encoding="utf-8" ?>

<collections>

  <collection name="CollectionName"
              pollingIntervalInSecs="60"
              initialState="running"
              saveData="yes"
              maxPollsPerDevice="50"
              deletePercentage="25">

     <table>
       <oid name="variableName1" dataLabel="Label/description" />
     </table>

     <table>
       <oid name="variableName2" dataLabel="Label/description" />
       <oid name="variableName3" dataLabel="Label/description" />
     </table>

     <scalar>
       <oid name="scalarVariable1" dataLabel="Label/description" />
       <oid name="scalarVariable2" dataLabel="Label/description" />
     </scalar>

     <scope ipAddress="123.234.345.456" />
     <scope ipAddress="123.234.345.789" />

  </collection>

</collections>
```

Within the outermost `collections` statement, you can define multiple individual collections, each bracketed with `<collection name= ... > </collection>`

The collection properties must be defined in the collection statement at the beginning of each collection definition:

Table 4: Control properties for a MIB collection specification

name	A name for the collection
pollingIntervalInSecs	The interval at which EPICenter should poll for the variables defined in this collection
initialState	Whether this collection should start running immediately upon loading (values are “running” and “stopped”)
saveData	Whether the collected data should be saved to the EPICenter database (“yes” or “no”)
maxPollsPerDevice	The maximum number of poll result sets that should be saved in the database
deletePercentage	The percentage of the saved data that should be deleted when the file reaches it specified limit

Table OIDs are defined in `<oid ... >` statements, included between `<table>` and `</table>` statements. OIDs from different tables must be put in separate `<table>` statements. The label portion of the statement appears in the MIB Collections Detail report, and as a heading in the exported data file.

Scalar OIDs are defined in `<oid ... >` statements included between a `<scalar>` and `</scalar>` statement.

The devices that should be polled are specified by IP address in `<scope ipAddress ...>` statements, one for each IP address.

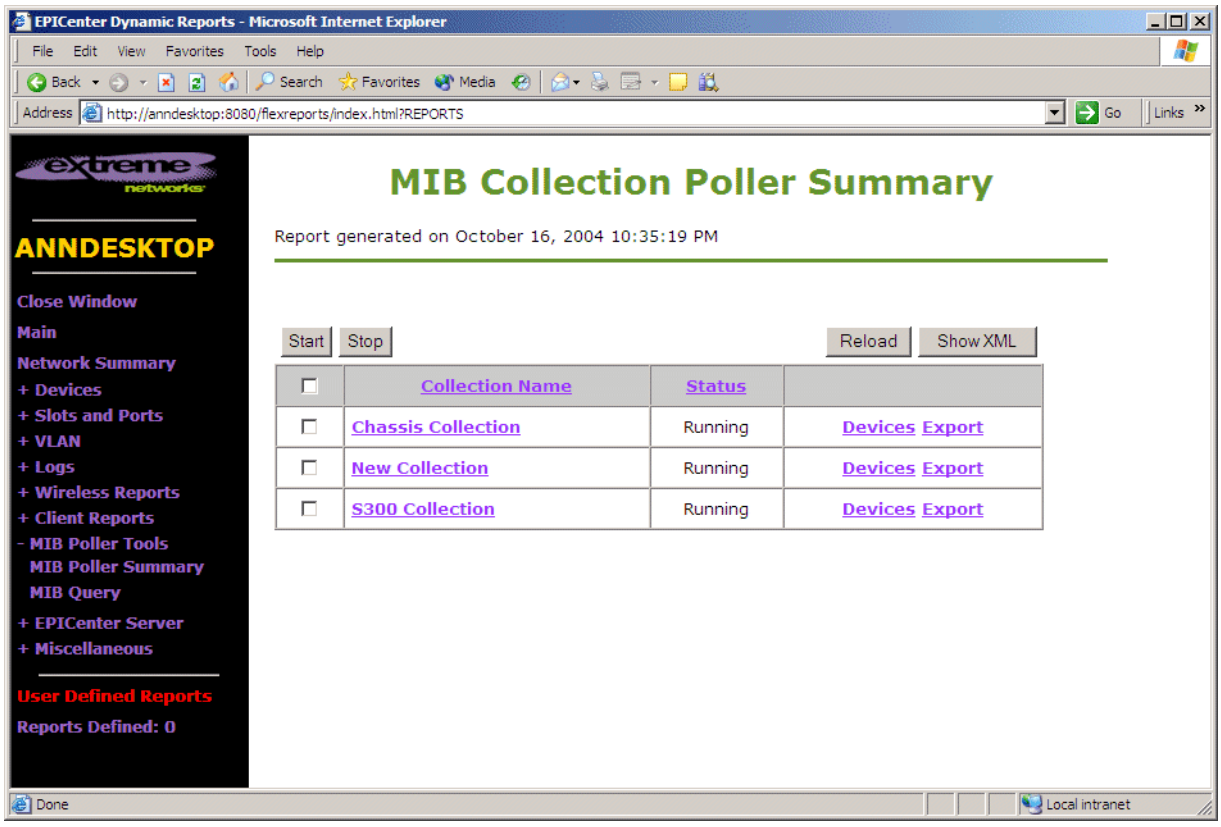
The completed file must be named `collections.xml`, and placed in the user/collections directory. The **Reload** button in the MIB Poller Summary report will load the collections.xml specification, and begin the collection process if the `initialState` property specifies "running."

Figure 56 on page 129 shows an example of an actual `collections.xml` file.

The MIB Poller Summary

If a `collection.xml` file has been loaded, the MIB Poller Summary shows the names of the collections defined in the xml file, along with their status (running or stopped). Figure 53 shows the summary for a a set of three collections.

Figure 53: The MIB Poller Collection Summary



From this page, any user can view the details of the collection, view information about the devices on which data is being collected, view the xml file that defines the collections, and export the current results of the collection.

An EPICenter Administrator can start or stop polling for any or all of the collections, and can reload the `collections.xml` file.

Loading, Starting and Stopping a Collection

If a file named `collections.xml` exists in the EPICenter server's `user/collections` directory when the EPICenter server is started, the collection definitions in the file are loaded automatically. Polling for the collections will be started if the initialState property specifies that the collection should be running.

If the EPICenter server is already running when the `collections.xml` file is placed in the collections directory, then you must click the **Reload** button to load the collection definitions.

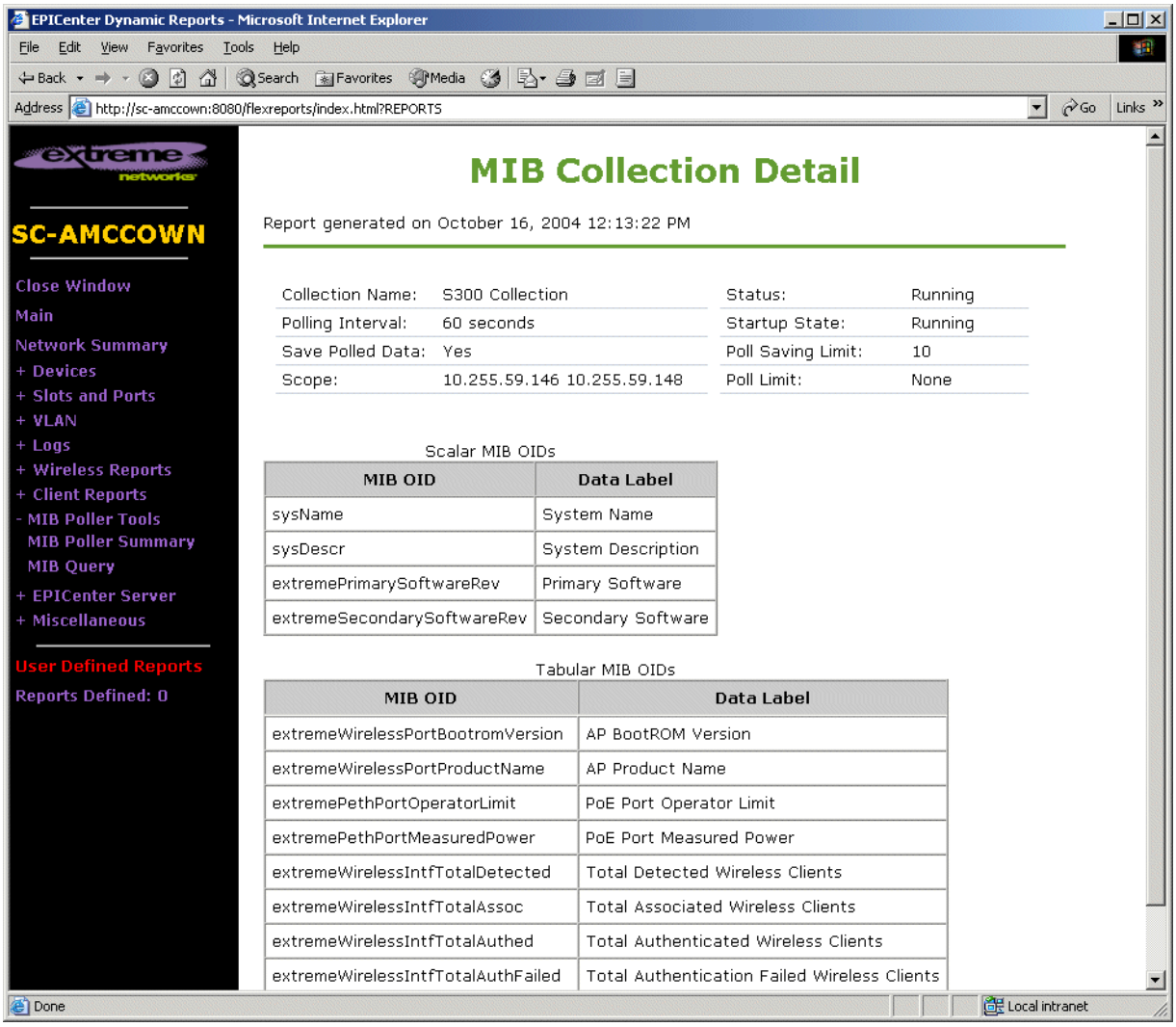
Once you have loaded the `collections.xml` file, the collections defined in that file will continue to be maintained, either running or stopped, until they are replaced by reloading the `collections.xml` file which has been modified to specify a different set of collections, or until the `collections.xml` file is removed from the collections directory.

You can stop the polling process for a running collection by placing a check in the checkbox in the first column next to the collection name, and clicking **Stop**. To start a stopped collection, check the box in the first column and click **Start**. You can select all the collections in the table by checking the box in the column heading.

The MIB Collection Detail Report

To view the details of a collection, click the collection name, which links to the MIB Collection Detail report for the collection. Figure 54 is an example of a Collection Detail Report.

Figure 54: MIB Collection Detail Report



The top area of the MIB Collection Detail Report shows the properties of the collection, as defined in the `collections.xml` file:

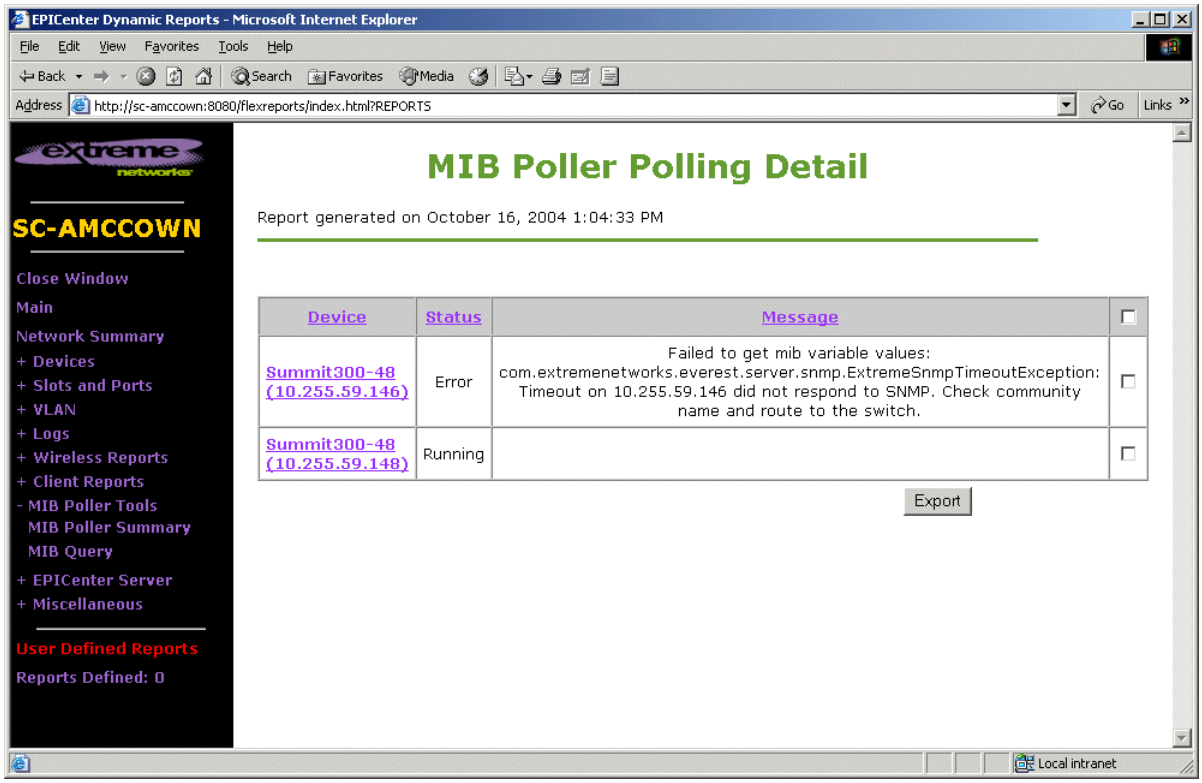
Collection Name	The name of the collection
Polling Interval	The polling interval, in seconds
Save Polled Data	Whether the polled data is being saved in the database (Yes or No)
Scope	The devices on which polling for this data is being conducted
Status	The status of the collection (running or stopped)
Startup State	Whether the poll should be started automatically when it is loaded (running) or should be left in the stopped state
Poll Saving Limit	The lower boundary of the number of poll results that will be saved in the database. This value is calculated by taking the maximum number of saved polls multiplied by the delete percentage. The actual number of poll data sets in the database at any given time will be somewhere between this value and the maximum poll saving limit.
Poll Limit	A limit on the number of polls that should be performed. Currently this is always None, the number of polling cycles cannot be limited at this time.

The two tables below show the scalar and tabular MIB variables (OIDs) for which polling will be done. Each variable is identified by its OID and the data label that was provided in the xml file.

The MIB Poller Detail Report

The Poller Detail report simply shows the status of the collection for each device in the collection scope.

Figure 55: MIB Collection Detail Report



This report shows the following information:

Device	The name of the device. This is also functions as a link to the Device Details report for the device
Status	The status of the collection on this device (running, stopped, or error)
Message	A message, if appropriate, explaining the status (such as an error message).

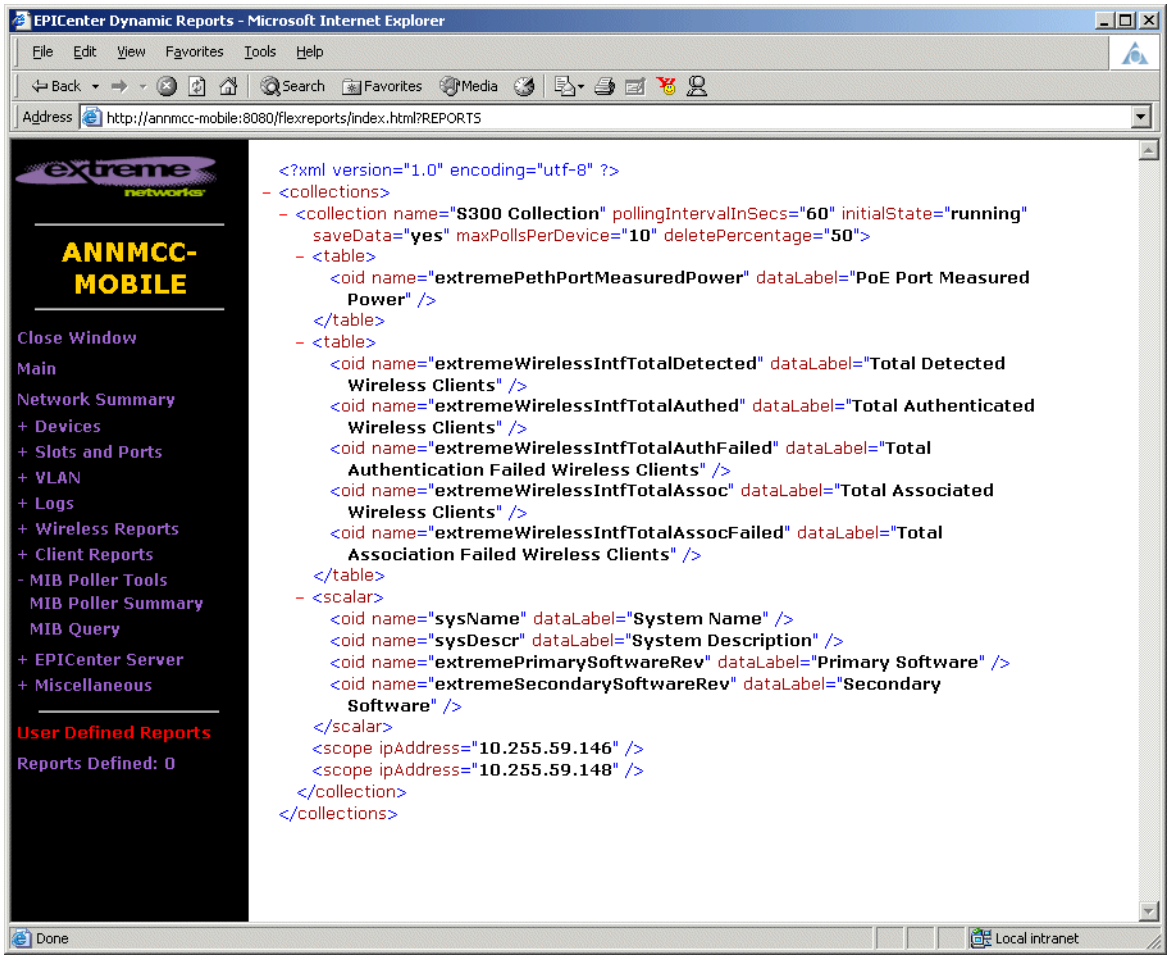
The last column provides checkboxes that can be used to select devices for which to export the collection results.

To export results for a device, click to check the appropriate box, then click the **Export** button below the table. You can select all devices by checking the box in the table header.

Viewing the XML Collection Definition

To view the collection definitions, click the Show XML button in the MIB Collection Poller Summary. This displays the XML that defines the currently loaded collections. Figure 56 show an example of the XML for a collection definition.

Figure 56: A MIB Collection definition shown in XML



Exporting the Collected Data

One of the main purposes for collecting historical MIB data over time is to allow analysis to identify trends or patterns that may provide insights into your network usage. In order to do this, you need to export the collected MIB data so it can be used by other analysis tools.

The MIB Poller Tool allows you to export data as comma separated text and save it to a file. You can export the data from either the MIB Collection Poller Summary report, or from the MIB POller Poling DEtail Report.

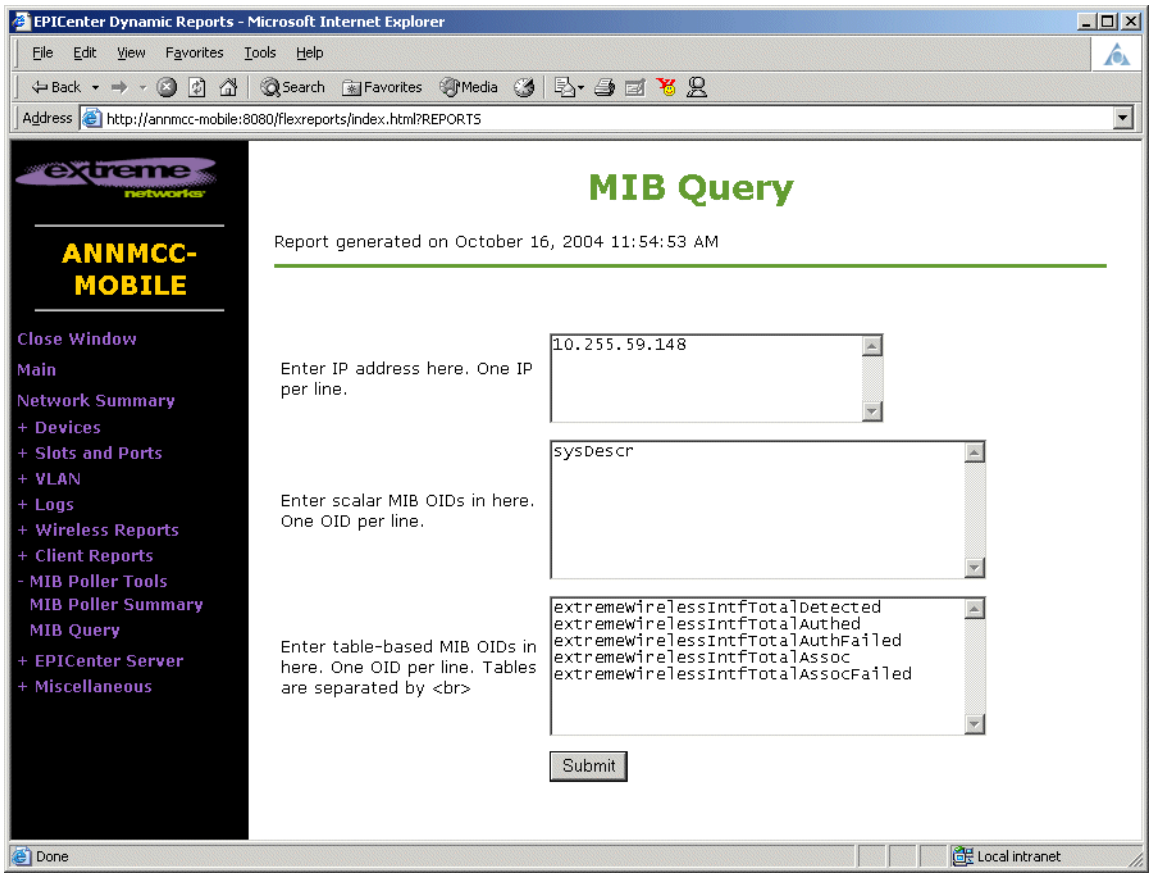
- From the MIB Poller Summary report, you can export the results for an entire collection— click the **Export** link in the row for the collection whose data you want to export. This exports the results for all devices in the collection into a single text file, and places the text file into a archive (zip) file.
- From the MIB Poller Polling Detail report you can export the results for individual devices in a collection. Check the checkboxes in the last column, then click the **Export** button. This exports the results for the selected devices into a single text file, and places the text file into a archive (zip) file.

Once exported, the text file can be imported into another application, such as a spreadsheet, for analysis.

The MIB Query Tool

The MIB Query Tool lets you retrieve the values of MIB variables on a one-time basis. It does not do any repeated polling, and does not store the results.

Figure 57: A MIB Query example



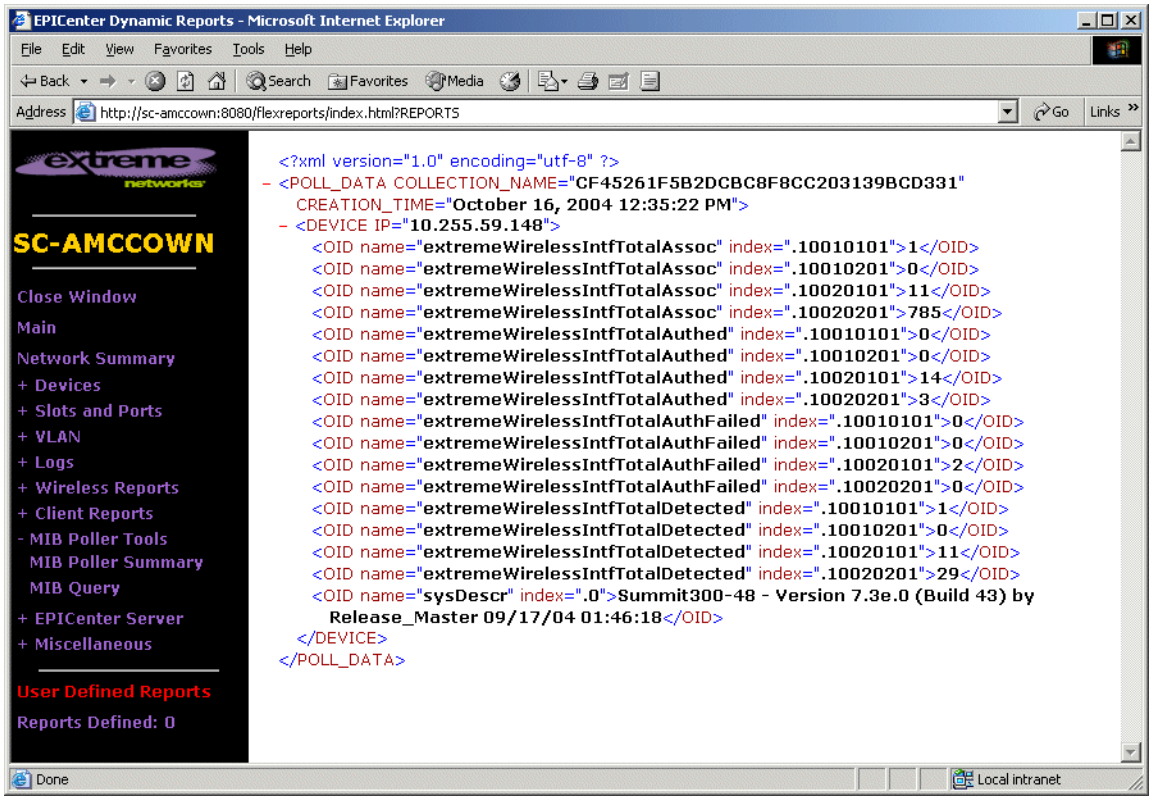
To perform a MIB query, you enter the required data into the appropriate fields:

- Enter into the first field the IP addresses of the devices from which you want to get data.
- Enter any scalar MIB OIDs you want to retrieve into the second field.
- Enter any Table-based MIB OIDs into the third field.

Entries must be one item per line.

Click **Submit** to execute the query. The results are returned in XML format in the reports window.

Figure 58: The results of a MIB Query



Reconfiguring EPICenter Ports

In some circumstances, the ports used by default within EPICenter may conflict with ports already in use on your system by other applications.

The Port Configuration Utility lets you change the default database server port and the default web server port without requiring you to re-install the EPICenter software. See the “Port Configuration Utility” on page 187 in Appendix B for details on using this utility.

It is also possible that you may need to change the ports used by the Tomcat server, if they conflict with those used by other applications.

To change these ports, you must edit the `server.xml` file found in the `tomcat\conf` directory under the EPICenter installation:

- In Windows this would be `\Program Files\Extreme Networks\EPICenter 5.0\tomcat\conf\server.xml`.
- In Solaris it would be `/opt/extreme/epc5_0/tomcat/conf/server.xml`

Look for the statement defining the Coyote Connector, as shown here:

```
<!-- Define a non-SSL Coyote HTTP/1.1 Connector on port 80 -->
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector" port="8080"
proxyPort="8080" minProcessors="5" maxProcessors="75" enableLookups="true"
redirectPort="8444" acceptCount="100" debug="0" connectionTimeout="20000"
useURIValidationHack="false" disableUploadTimeout="true" />
```

The two ports you can change are the one simply named **port** (set to 8080) and the **redirectPort** (set to 8444).

Using the EPICenter Debugging Tools

The EPICenter debugging tools are available through the Reports modules for users with an administrator role. You should not attempt to use any of these tools except under the direction of Extreme Networks Technical Assistance Center personnel.

This "report" provides links to the following tools:

- **Set logging level**: lets you set the Server Side Client Debug Level, and the Server Debug Level. This page also shows you the debug Telnet port number.
- **Check server internals**: This creates a report of server internal status.
- **Query Database**: Lets you enter an SQL query against the EPICenter database. This is for use only at the direction of Extreme Networks Technical Assistance Center personnel.

10 VoIP and EPICenter-Avaya Integrated Management

This chapter describes how the EPICenter software interacts with the Avaya Integrated Management software when the two servers are co-resident on the same system:

- Discovering devices managed by Avaya Integrated Management software
- Launching the Avaya Integrated Management Console and the Avaya Device Manager
- Monitoring IP Phone locations and status

Overview

The EPICenter/Avaya integration has been developed jointly by Extreme Networks and Avaya to deliver a set of tools that enable managing and troubleshooting Avaya Voice and Extreme Networks infrastructure networks in a coordinated manner. Each product can discover and display devices from the other vendor, and can cross-launch both the network management application (EPICenter or the Avaya Network Management Console) and device managers embedded in the supported devices.

NOTE

Avaya's Avaya Integrated Management 2.2 is supported on Windows 2000 and Windows 2003 Server; therefore, the Avaya/EPICenter integration is only supported in those two operating environments.

For information on Extreme Networks features available through the Avaya Integrated Management software, see the Avaya Integrated Management documentation.

When EPICenter is installed on the same server with the Avaya Integrated Management software, it can interact with the Avaya Integrated Management software in a number of ways:

- EPICenter supports the discovery and display of Avaya Media Servers, Media Gateways, and IP endpoints.
- The Avaya Network Management Console can be launched from within EPICenter
- The embedded Avaya Integrated Management device manager can be launched for a selected Avaya device.
- A single sign-on capability allows an Avaya Integrated Management user to be automatically logged into EPICenter when EPICenter is launched from the Avaya Integrated Management software. However, EPICenter users must provide a username and password in order to log into the Avaya Integrated Management Console or Device Manager.

- The IP phones in the Avaya Integrated Management Console inventory can be imported into EPICenter, and their location and status can be monitored from within EPICenter.

Support for these features requires that EPICenter and the Avaya Integrated Management software version 2.2 be co-resident on the same server. The Avaya Integrated Management software can be installed as a stand-alone application or as a plug-in to HP OpenView.

In EPICenter, the integration with the Avaya Integrated Management software adds the following features when the two servers are co-resident on the same system. These features are not available when the Avaya Integrated Management software is not co-resident:

- Discovery: an **External Discovery** radio button will enable EPICenter to retrieve the IP addresses of devices the Avaya Integrated Management Console is managing so that EPICenter can discover those devices. This button loads the IP addresses of the devices in the Avaya Integrated Management inventory into the discovery list so that they can be discovered by EPICenter.
- Discovered Avaya devices will be placed in the EPICenter Inventory database, will appear on Topology maps, and will be monitored in EPICenter as a third-party device.
- Three additional commands are available on the EPICenter Tools Menu:
  - AIM Console: launches the Avaya Network Management Console (not available if the Avaya Integrated Management software is installed as a plug-in to HP OpenView)
  - Import IP Phones: gets location and status information about IP phones connected to an Extreme Networks device
  - Sync IP Phones: updates location and status information for IP phones connected to an Extreme Networks device.
- On the right-click pop-up menus, when an Avaya device is selected, the Device Manager command can launch the Avaya Device Manager application on the selected device. If you are running the EPICenter client on the same system as the Avaya Integrated Management server, the Avaya Device Manager runs as an application; in all other cases the Avaya Device Manager runs in a browser window.

NOTE

The ability to launch the Avaya Device Manager can be disabled by an EPICenter administrator through the Avaya Integration properties in the EPICenter Admin feature.

- In the Properties display for an Extreme Networks device (accessed from the EPICenter display menu or from the right-click pop-up menu) an IP Phones tab is available. This tab shows the location, identity (MAC and IP addresses and extension if available) and status of any IP phones connected to the Extreme Networks device.
- An IP Phones report is available in the Reports feature that displays identification and status information for IP phones connected to Extreme Networks devices.
- In the EPICenter Admin feature, a set of properties is available specific to the Avaya Integration to enable or disable trap forwarding from EPICenter to the Avaya Integrated Management software.

Installation Considerations

The Avaya Integrated Management server and the EPICenter server must be co-resident on the same Windows 2000 or Windows 2003 system for the integration features to function. Installation of the

integration features is transparent, no extra steps are required in the installation process of either product. The order of installation does not matter.

- If the Avaya Integrated Management software is already present on the server system when the EPICenter server is started, the integration features (menu items etc.) will appear in EPICenter.
- If the Avaya Integrated Management software is installed on a system where a running EPICenter installation already resides, the EPICenter server must be restarted to recognize the Avaya Integrated Management integration features.

TFTP Server Coordination

Both EPICenter and the Avaya Integrated Management software provide TFTP servers, but only one run. To avoid problems, you should disable one of the TFTP servers, and configure the TFTP root to point to the enabled TFTP server.

To disable the TFTP server in EPICenter, do the following:

1. From either the Configuration Manager or the Firmware Manager, click the **TFTP** button on the Toolbar (or select TFTP from the Firmware or Config menus).

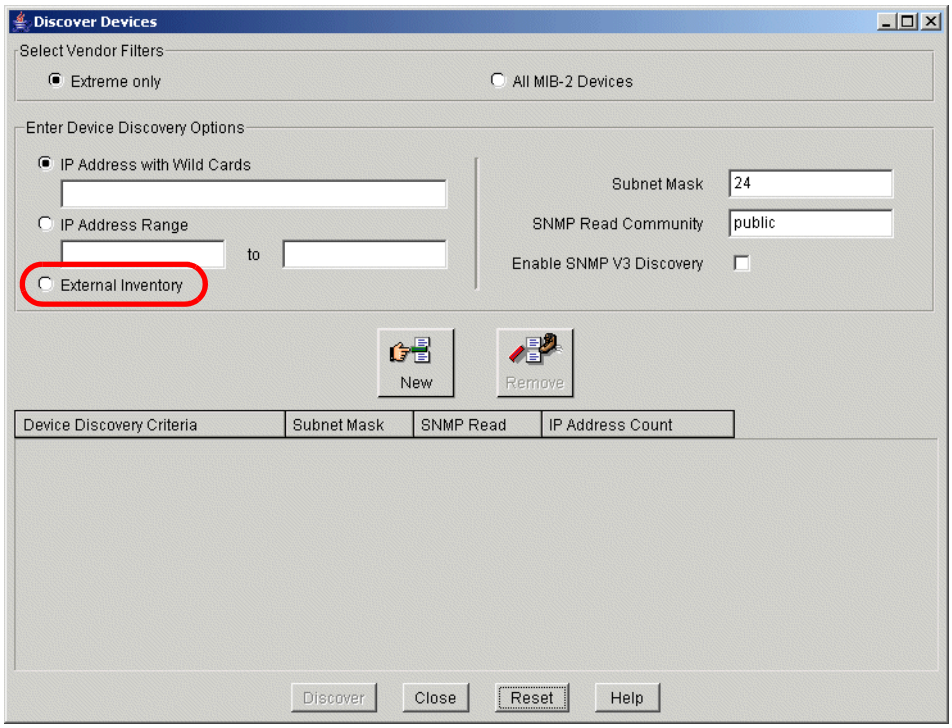
   The Configure TFTP Server dialog appears.
2. Click the Disable EPICenter TFTP Server radio button
3. Type the path of the Avaya Integrated Management server TFTP root directory
4. Click **Apply**.

Discovering Avaya Devices

Discovering Avaya devices works just like discovering Extreme Networks devices or other MIB-2 compatible devices.

1. From within the Inventory Manager, click the **Discover** button or select Discover from the Inventory menu.
2. When the Discover Devices window appears, instead of entering an IP address with wild cards or an IP address range, select **External Inventory**.

Figure 59: The Discover Devices window when the Avaya Integrated Management server is co-resident on the system



3 Select the **All MIB-2 Devices** checkbox to discover non-Extreme Networks devices.

4 Click **New**. EPICenter will query the Avaya Information Manager for the devices it is managing, and will add those to the list of IP addresses to discover.

5 Click **Discover**. The discovery will proceed as with any other discovery for a specific set of IP addresses.

6 Once the discovery has completed, you can add the Avaya network devices to the Inventory Manager database. The discovery typically discovers both Avaya network devices and Avaya IP phones.

NOTE

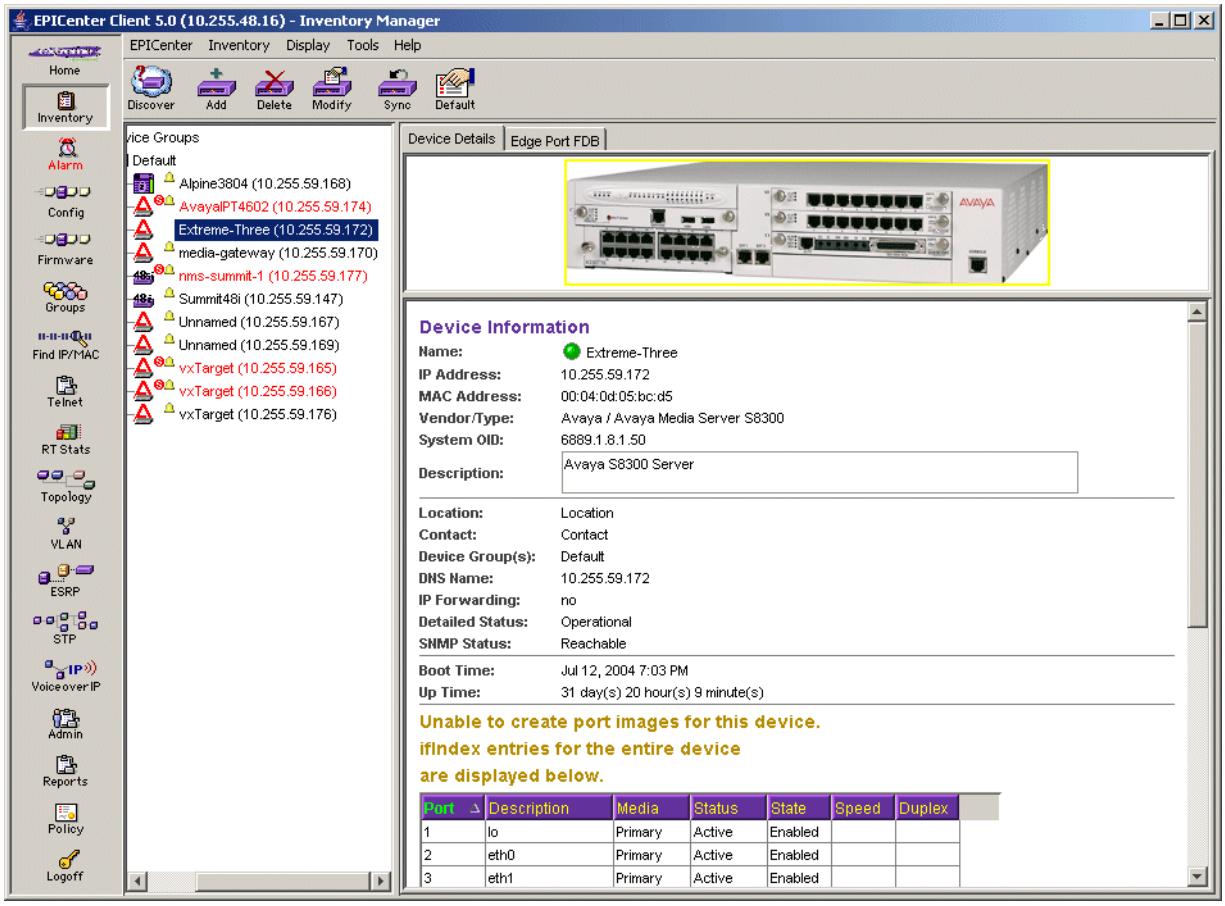
It is recommended that you NOT add Avaya IP phones into the EPICenter Inventory database. IP phones cannot be managed by EPICenter. If you add them to the Inventory database they will appear on EPICenter Topology maps and in the Component Tree, and they will be counted in the number of devices allowed under the terms of your EPICenter license agreement, even though they cannot be managed through EPICenter.

Avaya Devices in EPICenter

EPICenter manages Avaya devices as it manages other known third-party devices. It provides device images for the different types of Avaya devices in the Device Details view in the Inventory Manager.

Avaya devices are denoted in the Component Tree with an Avaya icon , as shown in Figure 60.

Figure 60: Device Details in the Inventory Manager for an Avaya device.



The Device sub-menu, accessed from the right-click pop-up menu or the Tools menu, provides a command to launch the device manager for the selected Avaya device. The device manager appears in a separate window, either running in a browser window or as a separate application depending on whether your EPICenter client is running on the same system as the Avaya Integrated Management and EPICenter servers.

Launching the Avaya Device Manager from the Devices Sub-Menu

In most EPICenter features, where you can select an Avaya device (either in the Component Tree, or from a feature such Topology map) you can use the Device sub-menu to launch the Avaya Device Manager for the selected Avaya device. The Device sub-menu is available from the Tools menu, or from a pop-up menu when you right-click on a selected device in the Component Tree.

The Avaya Device Manager runs as an application if the EPICenter client is running on the same system as the Avaya Integrated Management server. In all other cases the Avaya Device Manager runs in a browser window.

For information about using the Avaya Device Manager to manage an Avaya device, see the Avaya documentation.

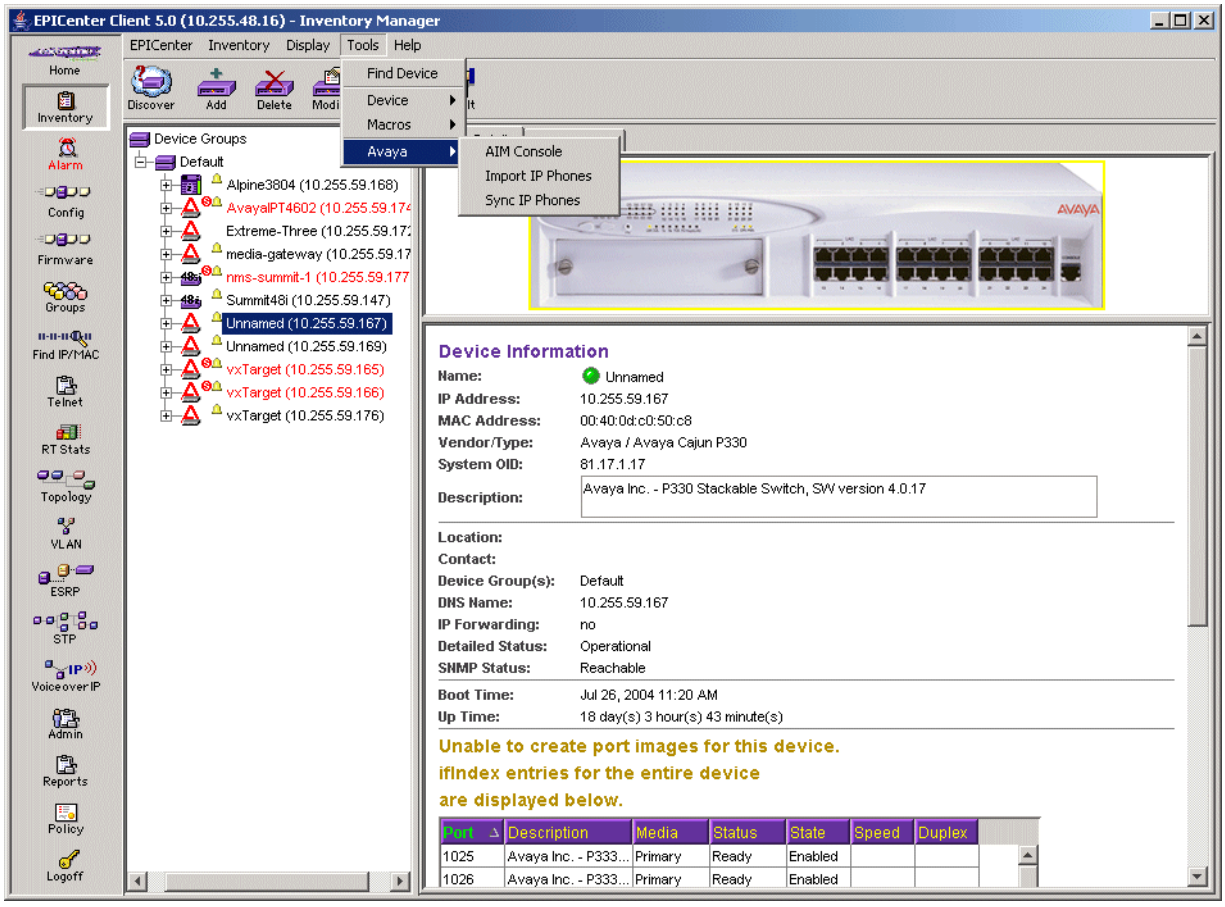
The Avaya Device Manager is normally launched through the Avaya Integrated Management Console. If necessary you can change this through the Avaya Integration properties in the Admin feature, so that

the embedded Device Manager is launched directly on the selected Avaya device instead of through the Avaya Network Management Suite.

Tools Menu Commands

When EPICenter detects that the Avaya Integrated Management server is co-resident on the system, it adds a submenu to the Tools menu specifically for Avaya.

Figure 61: The Avaya sub-menu on the EPICenter Tools menu.



The three Avaya-specific commands are:

Table 5: Avaya Sub-menu Commands on Tools Menu

AIM Console	Launches the Avaya Integrated Management Console. If your client is running on the same system where the EPICenter server and the Avaya Integrated Management server are installed, the Avaya Integrated Management Console runs as an application. If you are running the client on a different system than the EPICenter server and the Avaya Integrated Management server, then the Avaya Integrated Management Console is launched in a browser window. If the Avaya Integrated Management software is installed as a plug-in to HP OpenView, this command is not available.

Table 5: Avaya Sub-menu Commands on Tools Menu

Import IP Phones	Detects and imports MAC and IP address information about IP phones attached to the ports of the Extreme Networks devices known to EPICenter. See “Importing IP Phones” on page 139 for details.
Sync IP Phones	Uses MAC poller data to update information about IP phones connected to Extreme Networks devices. See “Syncing IP Phones” on page 141 for more information.

Launching the Avaya Integrated Management Console from EPICenter

As long as the Avaya Integrated Management server is installed directly on the same system as the EPICenter server (and not as a plug-in to HP OpenView) you can launch the Avaya Integrated Management Console from the EPICenter Tools menu (available from any feature within EPICenter. This runs the Avaya Integrated Management Console in a separate window, either as an application (if your EPICenter client and the Avaya Integrated Management server are on the same system) or in a browser window (if your EPICenter client is running on a separate system).

You are asked for a user name and password to log into the Avaya Integrated Management Console.

For information about using the Avaya Integrated Management Console to manage Avaya devices see the Avaya documentation.

Monitoring IP Phones on Extreme Networks Devices

If the EPICenter and Avaya Integrated Management servers are co-resident, you can import information from Avaya Integrated Management about the IP phones connected to devices in the network. For IP phones connected to Extreme Networks devices you can monitor their locations (ports) through the Device, Slot, or Port Properties displays for those devices. You can also view an IP Phones report using the Reports feature that shows you the identities, locations and status information for all the IP phones known to EPICenter.

If Avaya Integrated Management is not co-resident, these IP phones features are not available in EPICenter, even if IP phones are connected to Extreme Networks devices. Information about IP phone identity is kept by the Avaya Integrated Management server, and must be imported into EPICenter from the Avaya Integrated Management inventory.

Importing IP Phones

IP phone information is detected and stored in the Avaya Integrated Management server. This information is not available to EPICenter until you import it using the **Import IP Phones** command from the EPICenter **Tools** menu.

- To import IP Phones, click **Import IP Phones** under the Avaya sub-menu on the **Tools** menu at the top of the window.

The import function retrieves IP phone information from the Avaya Integrated Management server and stores it in the EPICenter database.

The import does not require any user input. A message box appears that shows the progress of the import action and reports on the total number of phones imported. When the import has completed, click **OK**.

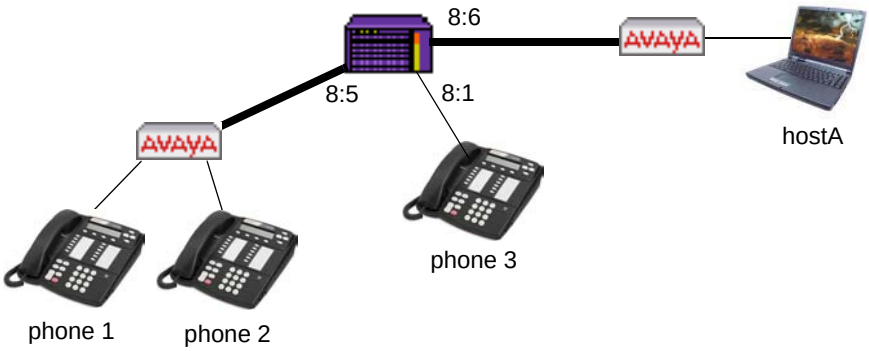
When the import is done, EPICenter will have a list of IP phone MAC addresses, along with IP addresses, extensions, and status, which are correlated with ports on Extreme Networks switches.

Although IP phone information (based on MAC Poller data) is kept in the EPICenter database, the phones are not included in the device inventory, and are visible only through the Properties display of the device to which the phones are connected, or through the IP Phones report. IP phones connected to Extreme Networks devices do not appear in the Component Tree or on any Topology maps.

IP Phone location and status data is based on information learned by the EPICenter MAC Poller. The MAC Poller collects MAC address and other information about the devices it detects on the edge ports of Extreme Networks devices. The MAC Poller determines whether a port is an edge port or a trunk port based on whether the port runs EDP.

For IP Phones connected directly to ports on Extreme Networks devices, the MAC Poller can accurately detect IP phone information. For IP phones connected to Avaya devices, however, the MAC Poller will only be able to detect the phone when it appears on a port on an Extreme Networks device. This can result in multiple phones appearing on a single port (the port connecting the Extreme device and the Avaya device), or a phone appearing on more than one port (if a second Avaya device contacts a phone on an Avaya device through an Extreme Networks device. Figure 50 shows an example of this:

Figure 62: IP phone connection scenario



In the scenario shown in Figure 62, phones 1 and 2 are connected to an Avaya system, which is connected to an Extreme Networks system via port 8:5. Because the link between the Avaya and Extreme systems does not run EDP, the EPICenter MAC Address Poller will see that link as an edge port, and will detect both phones 1 and 2 on port 8:5 on the Extreme Networks switch (assuming the phones have been active). Phone 3, which is directly connected to an edge port (8:1) on the Extreme Networks switch, will be correctly detected by the MAC poller.

Further, if hostA on the second Avaya system connects to phone 1, 2, or 3 (for example, pings one of those phones) then the MAC poller will also detect that phone on port 8:6.

If phones 1 and 2 remain inactive for a sufficient length of time their FDB entries will time out, the EPICenter MAC Address Poller will no longer find them, and they will no longer appear on either ports 8:5 or 8:6. Since port 8:6 is a trunk port, it is possible to disable FDB edge port polling through the EPICenter Inventory Manager for that specific port, which would prevent the phones from being detected on that port.

Syncing IP Phones

When an IP phone location has changed, the Properties display for the affected device(s) will reflect the new location, but the EPICenter database will continue to contain the outdated location information until you do a Sync IP Phones. The **Sync IP Phones** command uses MAC address information from the MAC poller to update IP phone information in the EPICenter database.

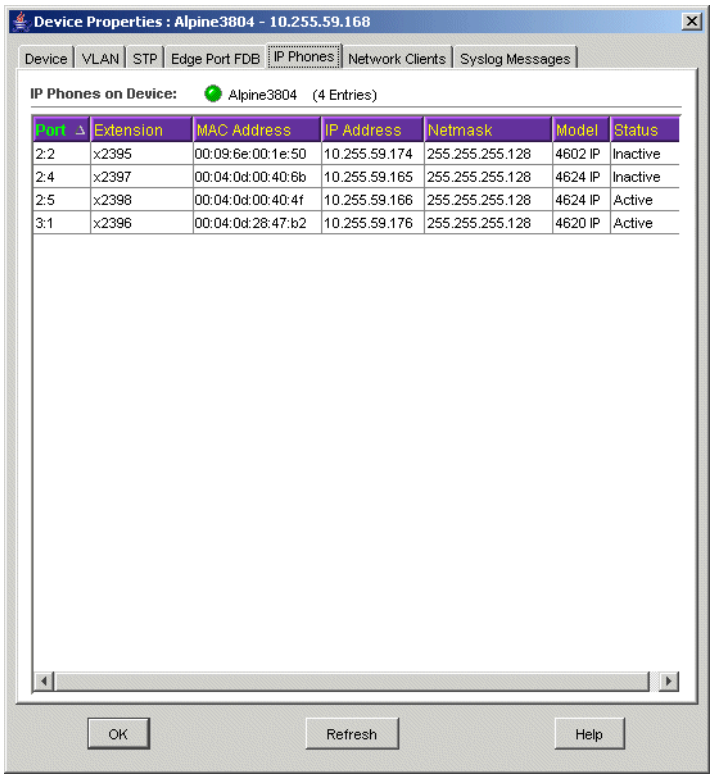
- To update IP Phone information in the EPICenter database, click **Sync IP Phones** under the Avaya sub-menu on the **Tools** menu at the top of the window.

As with the Import IP phones command, no user input is required—a message box shows the progress of the sync operation. When the Sync has finished, updated information can be viewed through the Properties displays or through the IP Phones report.

The IP Phones Properties Display

When EPICenter and the Avaya Integrated Management server are co-resident, an additional tab is present on devices that have IP phones connected. The **IP Phones** tab lists the IP Phones detected on the device, as shown in Figure 63.

Figure 63: The IP Phones tab of the Device Properties display.



The IP Phones tab shows the following information about the IP Phones on the device:

Port	The port on which the phone has been detected
Extension/IP Address	The phone extension, or the IP address (if the Avaya Integrated Management server is installed as a plug-in to HP OpenView, only the address is available, not the extension).
MAC Address	The MAC address of the IP phone set

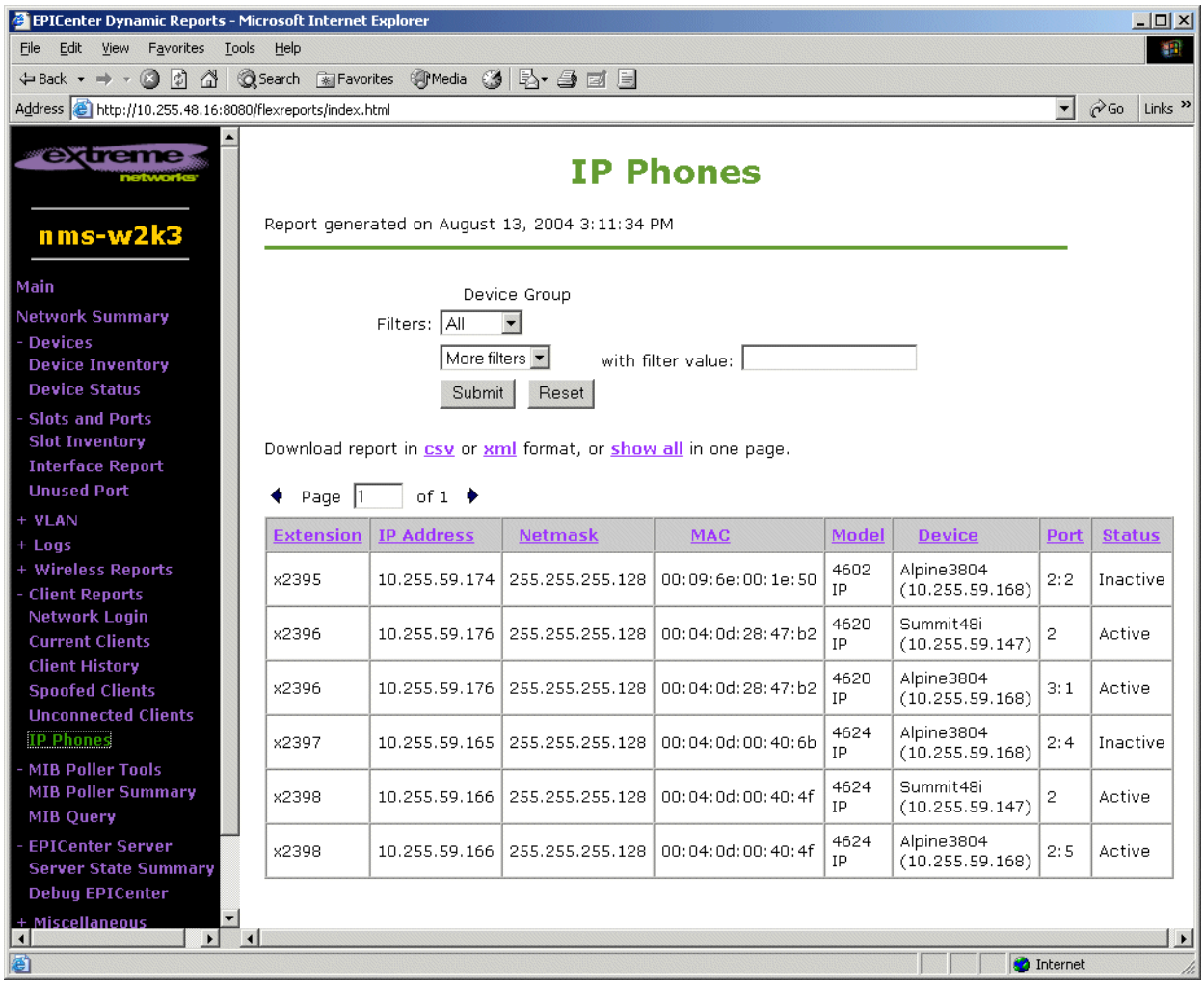
IP Address	IP address of the IP phone
Netmask	Subnet Mask for the IP phone
Model	The model (type) of IP phone
Status	The phone status: • Active: its MAC address is present in the device's operational FDB • Inactive: the MAC address is not present in the operational FDB.

This list will display the most current IP phones information; if a phone has been moved from one port to another, that will be reflected in this display. However, until you do a Sync operation, the EPICenter database will continue to contain outdated information.

IP Phones Reports

The IP Phones report shows the complete inventory of IP phones known to EPICenter. The report can be sorted based on any of the columns, and can be filtered by Device Group, and within Device Group by extension, or phone IP address.

Figure 64: The IP Phones report



The IP Phones report displays the following information about each phone:

Extension	The phone extension
Extension/IP Address	The phone extension, or the IP address (if the Avaya Integrated Management server is installed as a plug-in to HP OpenView, only the address is available, not the extension).
Netmask	Subnet Mask for the IP phone
MAC	The MAC address of the IP phone
Model	The model (type) of IP phone
Device	The device on which the phone has been detected
Port	The port (or slot and port) on which the phone has been detected
Status	The phone status: • Active: its MAC address is present in the device's operational FDB • Inactive: the MAC address is not present in the operational FDB.

Click the heading of a column to sort on the contents of that column.

To filter by Device Group, select the Device Group from the drop-down list in the top **Filters:** field, then click **Submit**.

To filter by Extension or by the IP address of the phone, select the appropriate setting from the second drop-down field, enter the value to be matched (a specific extension or IP address) in the **with filter value:** field, then click **Submit**.

Click Reset to reset the filter properties to the default (All Device Groups, no other filtering).

See Chapter 16, "Dynamic Reports" in the *EPICenter User Reference Guide*, or refer to the online Help for more information on working with reports.

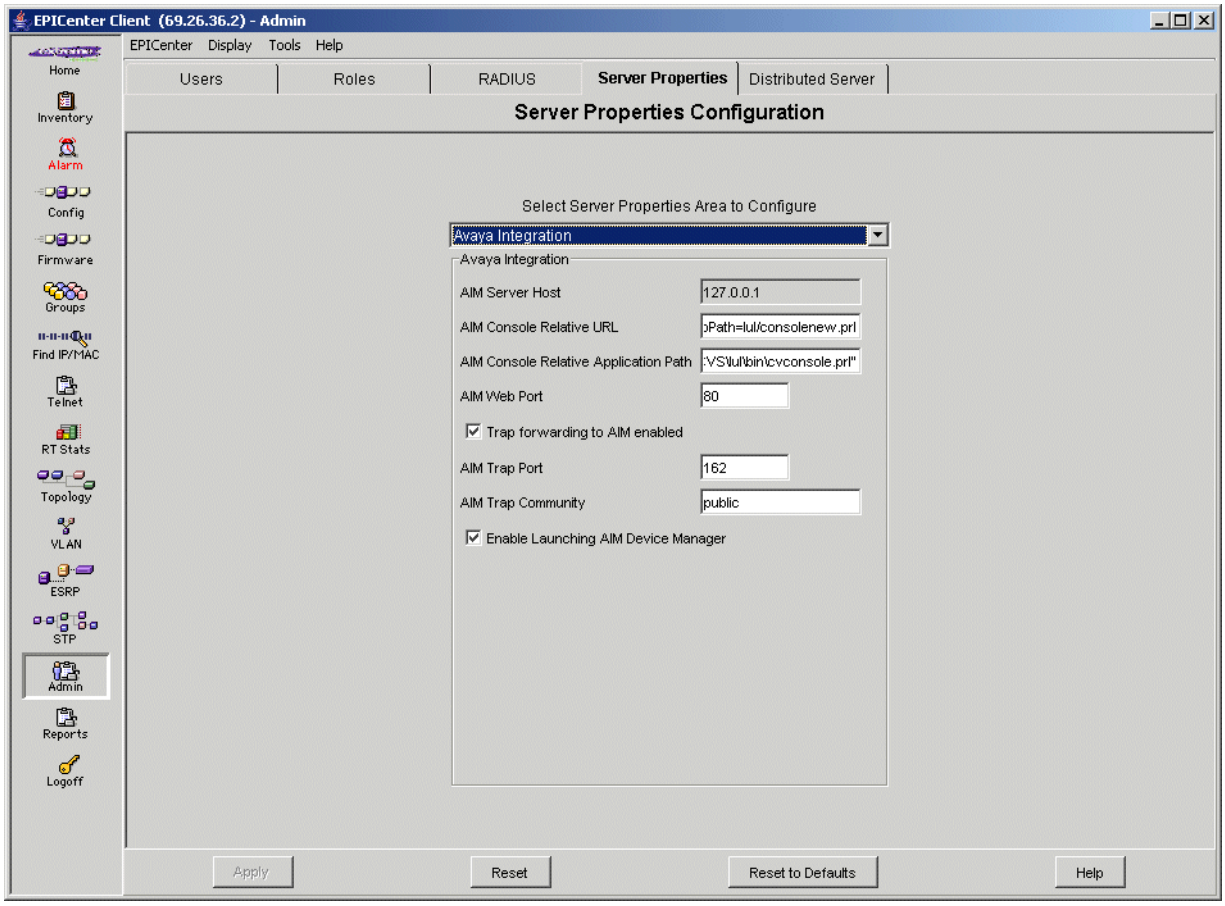
EPICenter System Properties for Avaya Integration

If you are an EPICenter Administrator (have an Admin role) there are several properties you can set through the EPICenter Admin applet that control aspects of the EPICenter/Avaya integration. Through the Avaya Server properties you can set:

- The Avaya Integrated Management server host IP address, the URL for the Avaya Integrated Management console, and the port for the Avaya Integrated Management server's web server
- Whether traps should be forwarded to the Avaya Integrated Management server, and if so, the trap port and trap community string
- Whether the Avaya Device Manager should be able to be launched from EPICenter.

Figure 65 shows the Server Properties you can set under the Avaya Integration category.

Figure 65: The Avaya Integration Server Properties, Admin feature



When you select Avaya Integration from the drop-down menu field at the top of the Properties panel, you can set the following properties:

AIM Server Host	The IP address (or host name) of the system running the Avaya Integrated Management server. ***Note:*** In EPICenter 5.0 this must be the local host (127.0.0.1 or localhost).
AIM Console Relative URL	Relative URL of the Avaya Integrated Management Console. This is used to launch the Avaya Integrated Management Console in a browser window.
AIM Console Relative Application Path	Relative path to the Avaya Integrated Management Console executable. This is used to launch the Avaya Integrated Management Console when the EPICenter client is running on the same system as the Avaya Integrated Management and EPICenter servers.
AIM Web Port	The port used to communicate via HTTP with the Avaya Integrated Management web server. Default is 80, which is the Avaya Integrated Management server default. If the Avaya Integrated Management web server uses a different port, you must reconfigure this setting to match, or EPICenter will not be able to communicate with the Avaya Integrated Management web server.
Trap forwarding to AIM enabled	A check in this box indicates that trap forwarding from EPICenter to the Avaya Integrated Management server is enabled. The default is enabled.
AIM Trap Port	The port to which EPICenter should send traps. Default is port 162, which is the default used by the Avaya Integrated Management Console. If this port has been reconfigured for the Avaya Integrated Management Console, you must reconfigure this setting to match, or trap forwarding will not succeed.

AIM Trap Community	The community string EPICenter should use when fowarding a trap. If the community has been reconfigured in the Avaya Integrated Management Console, you must reconfigure this setting to match.
Enable Launching AIM Device Manager	A check in this box indicates that EPICenter will launch the Avaya Device Manager through the Avaya Integrated Management Console. Uncheck this box to launch the embedded Device Manager directly on Avaya devices by connecting directly to the IP address of the device via HTTP.

Launching EPICenter from the Avaya Integrated Management Console

One of the features of the EPICenter/Avaya integration is the ability to cross-launch one application from the other. The launch of the Avaya Integrated Management Console has been discussed in "Launching the Avaya Integrated Management Console from EPICenter" on page 139. You can also launch EPICenter from within the Avaya Integrated Management software.

EPICenter can be launched from within the Avaya Integrated Management Console in the context of a specific Extreme Networks device. This will launch EPICenter and will display the Inventory Manager Device Details view for the device selected within the Avaya Integrated Management Console.

The EPICenter/Avaya integration provides single sign-on, so when EPICenter starts, the Avaya user will be logged in automatically to EPICenter, assuming he/she is a known user. If the user cannot be recognized, the user will be mapped to one of the default EPICenter users ("admin" or the read-only "user") depending on the user type in the Avaya Integrated Management software.

If EPICenter is launched for a device that is not currently in the EPICenter inventory, a warning dialog is displayed. The user will then be able to use the External Inventory feature of Discovery to discover devices managed by the Avaya Integrated Management Console.

11 Policy Manager Overview

This chapter describes:

- An overview of the Policy Manager features
- An introduction to the concepts that are fundamental to creating policies using the EPICenter Policy Manager

Overview of the Policy Manager

Policy-based management is used to protect and guarantee delivery of mission-critical traffic. A network policy is a set of high-level rules for controlling the priority of, and amount of bandwidth available to, various types of network traffic. Using EPICenter, policies can be defined in terms of individual users and desktop systems, not just by IP or MAC addresses, ports, or VLANs.

The EPICenter Policy Manager lets you work with high-level policy components (users, desktop systems, groups of users or systems, applications, and groups of devices and ports) in defining policies. The policy system translates those policy components into the specific information needed for QoS configuration of network devices. It also detects overlaps and conflicts in policies, with precedence rules for resolving conflicting QoS rules.

NOTE

The EPICenter policy system is based on the policy-based QoS capabilities in the ExtremeWare software. For details on the capabilities and implementation of QoS in Extreme Networks switches, see the ExtremeWare Software User Guide or the ExtremeWare Release Note for the version(s) of the software running on your switches.

The EPICenter Policy Manager is a separately-licensed component of the EPICenter product family. When a Policy Manager license is installed on the EPICenter server, the Policy icon appears in the Navigation Toolbar at the left of your browser window.

If no icon is present, it indicates that no current license can be found for the Policy Manager module. See the *EPICenter Installation and Upgrade Note* or the *EPICenter Release Note* for information on obtaining and installing a license.

The EPICenter Policy Manager is organized into two functional areas.

- The Policies View, where you can create, view, and modify EPICenter policy definitions for Extreme Networks devices. The organizing principle within the Policies view is the policy definition.
- The ACL Viewer, where you can view the access list and QoS rules generated by the Policy Manager for the devices in your network. You cannot modify EPICenter policy definitions from within this view. The organizing principle within the ACL Viewer is the network device.

From either the Policies View or ACL Viewer, you can modify the QoS profiles, change policy precedence, and configure the currently-enabled policies on one or more devices.

The Policy Manager is closely tied to the EPICenter Grouping applet, which is used to define the network resources that can be used as traffic endpoints or to specify the policy scope in a policy definition. Resources must be set up through the Grouping Manager or Inventory Manager before you can use them in a policy definition. You should be thoroughly familiar with the Grouping applet before you begin to define policies using the Policy Manager.

Basic EPICenter Policy Definition

A QoS policy in the EPICenter Policy Manager is composed of the following components:

- A **Name** and **Description** that you supply when you create the policy. The **Description** is optional.
- The **Policy Type,** which translates to the implementation type (Access-based Security QoS, IP QoS, Source Port QoS, or VLAN QoS). The implementation type determines the type of traffic grouping the switch will look for in implementing the policy. This in turn determines what type of endpoints are allowed in your traffic definition, and how some of the other elements, such as traffic direction, are handled.
- A definition of the **Access List** (for Security policies) or **Policy Traffic** (for IP policies) to be affected by the policy. You define the policy traffic by specifying the endpoints the switch should use to identify the traffic of interest. The EPICenter Policy Manager lets you define the endpoints using a high-level set of resources described below (see “Policy Named Components” on page 156 for more details).
- The **Access Domain** or **Scope** of the policy—the set of network devices on which to apply the policy.
- The EPICenter Policy Manager converts the high-level policy definition you create into a set of low-level ACL and QoS rules that it will configure on the devices within the scope or domain of the policy. To do this, the Policy Manager takes the following steps:
  - **a** Converts the endpoint components and the specified traffic direction into traffic patterns.
  - **b** Uses the policy domain or scope to determine the device(s) and ports on which the QoS rules should be implemented.
  - **c** Determines the QoS profiles to associate with the traffic flows for each device in the scope.
  - **d** Resolves any QoS rule conflicts using precedence relationships.
  - **e** Configures the QoS rules on the network switches either automatically (if Auto Configuration is enabled) or when you initiate the configuration using one of the directed configuration operations.

Policy Types

The EPICenter Policy Manager supports four types of policies: Access-based Security QoS policies, IP QoS (Access List) policies, Source Physical Port QoS policies, and VLAN QoS policies. These policies assign QoS profiles to traffic flows that are identified based on dynamically determined destination port, IP-based endpoint addressing information, physical port of origin, or VLAN origin. This release of the EPICenter Policy Manager does not support policies for traffic based on MAC address destination information or on explicit class of service (802.1P and DiffServ) information.

ExtremeWare versions 5.0 or later support IP, VLAN and source port types. Only ExtremeWare 7.0 supports Security policies. ExtremeWare versions prior to 5.0 support only VLAN-based QoS. Thus, although the Policy Manager supports IP, Access-based Security, and Source Port policies, non-*i*-series devices will not be able to use those policies unless they are running ExtremeWare version 5.0. The Policy Manager will not attempt to configure policies on devices that cannot support them.

In the EPICenter Policy Manager, each policy type acts somewhat like a template, allowing you to specify only components that are valid for the policy type. For example, the Policy Manager expects you to enter two sets of endpoints for a Security or an IP policy, but only a single set of endpoints for a VLAN or Source Port policy. In addition, the Policy Manager will only show endpoints of valid types in the Select Policy Traffic list in the Edit Policy, Network Resource, Server, Clients or Users Endpoints windows.

Access-based Security Policies

Access-based Security Policies represent a new policy type similar to IP policies. They are dynamic policies which are designed and typically implemented at the edge of the network to enforce user based security on an IP basis whenever and wherever the user connects. The principal difference is that the ACL rules associated with the policy are dynamically applied to and removed from the network in response to network login and 802.1x login and logout events. The IP addresses are static in nature and determined by the network resources. The device port the user logs on dynamically determines the user IP addresses. In addition, unlike IP policies, security policies are applied only on the device through which the user logged on. These policies operate in concert with the currently defined static policies and other access-based security policies and share the same precedence properties.

You use Access-based Security policies for a number of important reasons. One primary function of these policies is to protect core network resources by controlling and enforcing security for user access at the point of entry to the network (e.g. edge network devices). Additionally, these policies allow you to augment the basic yes/no security provided by Netlogin with a finer grain control of access levels. Users can be granted or denied access to certain areas of the network and users can be given different service level guarantees by the use of different QoS profiles.

You also use Access-Based Security policies to grant various levels of service on a per user or user group level. By using different QP assignments on a per user or user group basis in the access domain of the security policy, each user receives a specific level of service on the edge device port. Static IP policies should be defined in conjunction with dynamic user policies to establish a baseline security access level and QoS level for all users. Typically, these static IP policies would be used to deny access to sensitive network resources and/or to provide a base level quality of service. These static IP policies should have lower precedence than the dynamic user based security policies to allow the dynamic user based security policies to override the static IP policies on a per user basis.

Access-based Security policies are implemented with dynamic ACL allocation/deallocation on a per edge device port basis by the policy server based on current users on the network. The ACL rules are only applied to the single edge device port in the access domain on demand upon user network login

(netlogin / 802.1x). This differs from the static IP, VLAN and source port policies which apply the ACL rules in a persistent manner on devices specified by the policy scope.

In the EPICenter Policy Manager, the endpoints of the traffic flow for Access-based Security policies are defined as one or more services and users. The EPICenter Policy Manager lets you specify the endpoints using named resources, such as user names or host names, or groups that include such resources. If you specify a group resource as an endpoint, only the resources within the group (and its subgroups) that can be mapped to an IP or subnet address will be used as policy endpoints on the network services side.

The default traffic direction for Access-based Security policies is user to network resource(s), which creates ACL rules with the source IP address as the user's IP address and the destination IP address as the network resource IP addresse. This secures the network as the user is denied or permitted access to the network resource(s). The bidirectional traffic setting is used when security policies grant access and additionally provide quality of service. The quality of service for the traffic between the user and the network resource(s) can be prioritized and guaranteed by the assignment of a specific quality profile on a per user basis.

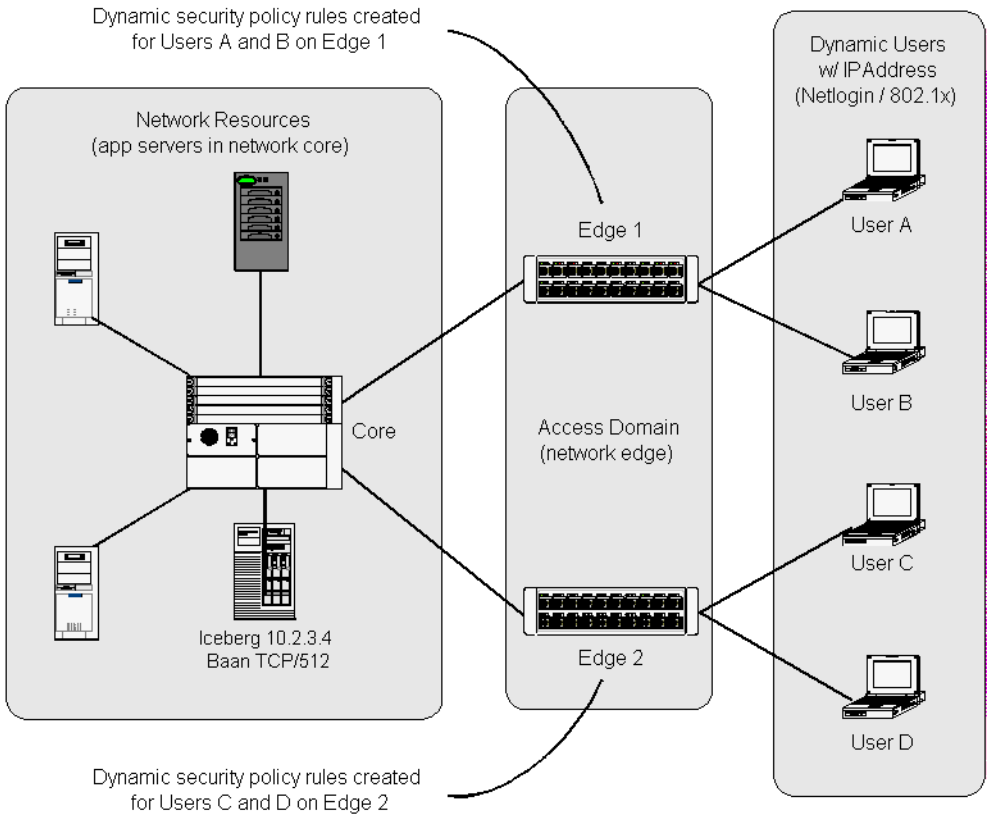
You can also further define the network resource-side traffic endpoints by specifying a named application or service, which translates to a protocol and L4 port, by directly specifying a protocol and L4 port range, or by using the Custom Applications group to collect a series of protocols and ports under one application. The EPICenter Policy Manager currently supports TCP and UDP as L4 protocols. In some cases you can also specify client-side L4 ports. The ICMP protocol is not currently supported.

The Policy Manager determines the traffic flows of interest based on the combination of endpoints and direction you have specified, and creates a set of IP QoS rules that can be implemented on the appropriate edge device (the login device).

Figure 66 shows the effects of a uni-directional Access-based Security policy specified between server Iceberg and users A, B, and C. The policy domain includes only the two rightmost switches. The effect of this policy is that Access-based Security QoS rules are implemented for one traffic flow through the upper switch and two through the lower switch, from Users A, B and C to the server called Iceberg. No rules are implemented on the intervening switches.

Although not shown in this diagram, you can specify multiple servers as well as multiple users.

Figure 66: Access-based QoS policy



An Access-based Security policy specifies traffic flow between two endpoints, one of which is dynamically determined when the user logs in on the network. The policy is applied only at the entry point to the system and does not need to be specified on each possible internal device that might be in the path for that policy. This reduces the policy load on the rest of the system. On the contrary, for an IP policy, the policy must be specified on each intermediate device in the path between the endpoints.

The EPICenter Policy Manager lets you specify the policy traffic flow in terms of named components. Therefore, you can specify server “Iceberg” as the server endpoint, and users “A,” “B,” and “C” as user endpoints. In addition, you can indicate that the traffic from the server should be filtered only to include traffic generated by the Baan application, which translates to TCP traffic originating from L4 port 512. Ports are not specified for the users.

More details of the traffic flow can be seen in the following sections.

IP-Based Policies (Access List Policies)

An IP-based policy identifies IP traffic flowing between specific source and destination endpoints, and then assigns that traffic to a QoS profile. For IP QoS, the traffic of interest is identified using any combination of IP source and destination addresses, layer 4 protocol, and layer 4 (L4) port information.

In the EPICenter Policy Manager, the endpoints of the traffic flow are defined as one or more servers and clients. The EPICenter Policy Manager lets you specify the endpoints using named resources such as user names or host names, or groups that include such resources, as long as they can be mapped to

an IP address. If you specify a group resource as an endpoint, only the resources within the group (and its subgroups) that can be mapped to an IP or subnet address will be used as policy endpoints.

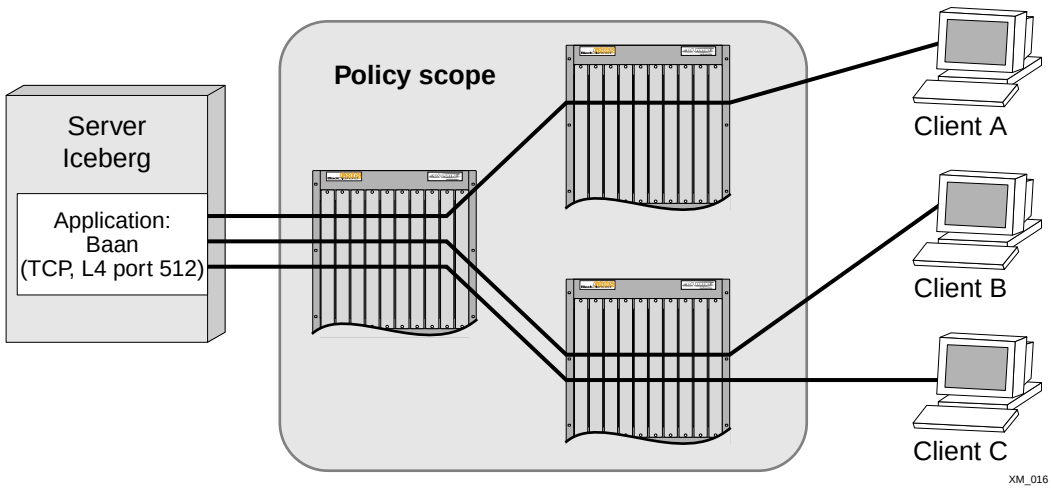
You can also further define the server-side traffic endpoints by specifying a named application or service, which translates to a protocol and L4 port, or by directly specifying a protocol and L4 port range. The EPICenter Policy Manager currently supports TCP and UDP as L4 protocols. In some cases you can also specify client-side L4 ports. The ICMP protocol is not currently supported.

The Policy Manager determines the traffic flows of interest based on the combination of endpoints and direction you have specified, and creates a set of IP QoS rules that can be implemented in the appropriate network devices.

Figure 67 shows the effects of a bi-directional IP policy specified between server Iceberg and clients A, B, and C. The policy scope includes all three switches. The effect of this policy is that IP QoS rules are implemented for six traffic flows on each switch: from the server to each of the three clients, and from each client to the server.

Although not shown in this diagram, you can specify multiple servers as well as multiple clients.

Figure 67: IP QoS policy



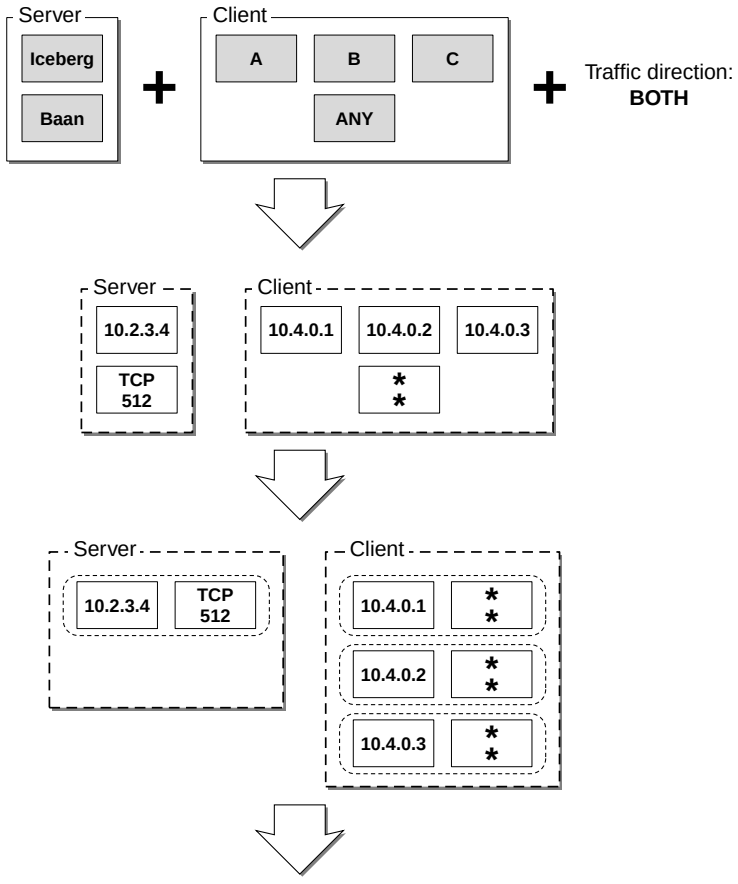
Unlike the VLAN and source port policy types, Security and IP policies specifies a traffic flow between two endpoints, and that traffic may travel through multiple network devices between those two endpoints. Thus, to protect the specified traffic along the entire route, the policy should be implemented on all the devices between the two endpoints. This is done by including these devices in the policy scope. On each device along the route, the traffic is identified based on the endpoint definitions (the IP address, protocols, and L4 ports), and is assigned to the specified QoS profile on that device.

The diagrams shown in Figure 68 illustrate how the traffic flows are generated for the example shown in Figure 67.

The EPICenter Policy Manager lets you specify the policy traffic flow in terms of named components. Therefore, you can specify server “Iceberg” as the server endpoint, and clients “A,” “B,” and “C” as client endpoints. In addition, you can indicate that the traffic from the server should be filtered only to include traffic generated by the Baan application, which translates to TCP traffic originating from L4 port 512. Ports are not specified for the clients.

Because they were defined through the EPICenter Grouping Manager, the Policy Manager can translate these high-level server and client names to IP addresses. Based on this information as well as the specified traffic direction, the Policy Manager generates the set of traffic flows shown in the table at the bottom of Figure 68. The diagram shows the steps involved in translating from the high-level objects (host name and service) to IP addresses and L4 ports and protocols, to a set of traffic flows used in policy rules.

Figure 68: Translation of a client/server policy definition into traffic flows



Destination IP	Destination L4 port	Source IP	Source L4 port
10.2.3.4	TCP 512	10.4.0.1	*
10.2.3.4	TCP 512	10.4.0.2	*
10.2.3.4	TCP 512	10.4.0.3	*
10.4.0.1	*	10.2.3.4	TCP 512
10.4.0.2	*	10.2.3.4	TCP 512
10.4.0.3	*	10.2.3.4	TCP 512

XM_017

Note that the potential number of traffic flows can get very large if you specify a large number of endpoints for both servers and clients. For “n” servers and “m” clients, the number of traffic flows affected by the policy will be **m*n**. For this reason, the use of subnets rather than large numbers of individual unicast IP addresses is recommended, when possible, for IP policies that involve multiple endpoints.

When both subnet and unicast IP addresses are in the endpoint, the Policy Manager determines the minimum set of IP/subnet addresses that are needed to represent all the addresses in the endpoint

specification. For example, if you specify policy endpoints as 10.2.0.0/16, 10.2.0.1, and 10.2.0.25, the Policy Manager will use only 10.2.0.0/16

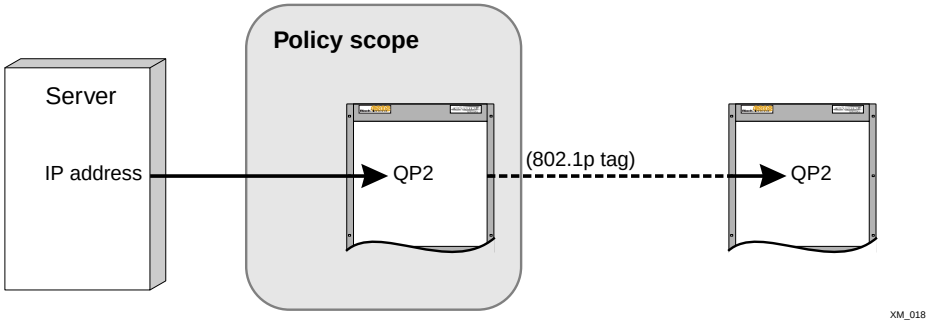
The IP QoS rules generated from EPICenter IP policy definitions are also known as Access List rules, because they define and control IP-based access between endpoints. A rule implementing IP-based QoS between server A and client B effectively defines the access allowed between those two endpoints. Access rules intended to permit access between the endpoints are implemented using one of the QoS profiles (QP1 through QP4 or QP8) that allow access, within the bandwidth and priority constraints defined by the QoS profile. An access rule intended to deny access from one endpoint to another is implemented in the EPICenter Policy Manager using the "blackhole" QoS profile.

IP-based QoS policies (or Access List policies) are supported on Extreme devices running ExtremeWare 5.0 or later— all *i*-series devices, and non-*i*-series devices running ExtremeWare 5.0x. This means that all devices in the scope for an IP policy must be running ExtremeWare 5.0 or later.

Source Port Policies

A Source Port policy identifies traffic originating from a specific port on an Extreme switch, and assigns that traffic to a QoS profile. In the policy definition, you specify as endpoints the specific ingress ports from which the traffic will originate. As shown in Figure 69, a source port policy is always uni-directional and implements Source Port QoS on the traffic flow from the specified source port.

Figure 69: Source Port policy



You can specify multiple source ports in a single policy, and you can specify them by providing higher-level resources such as a host name, user name, or a group, as long as the resources can be mapped by the Policy Manager to a port on a switch. If you specify a group, only the resources within the group (and its subgroups) that map to source ports will be used as policy endpoints.

In the case of source port QoS, the endpoint specification and the scope are theoretically redundant, because the endpoint specification effectively defines the scope of the policy. However, you must specify both the endpoint and the policy scope. If there are devices in the policy scope (for example, when the scope resource is a group) that are not related to the ports specified as endpoints. These will not be affected by the source port policy definition. For more details, see "Policy Access Domain and Scope" on page 159.

Unlike IP QoS, a Source Port QoS rule is implemented only on the device where the source port resides. However, you can enforce QoS throughout the network using 802.1Q tagging—specifically by explicit packet marking using 802.1p or DiffServ. If the switch ports used for output use 802.1Q tagging, the QoS profile assignment will be carried via the 802.1p priority bits to the next switch. On *i*-series chipset devices, you can also enable DiffServ examination and replacement to observe and carry the QoS setting with the packet between switches. The use of 802.1p priority bits is enabled when you enable tagging,

which you can do using the EPICenter VLAN Manager applet. DiffServ examination must be enabled using the ExtremeWare CLI or through ExtremeWare Vista. See the *ExtremeWare Software User Guide* for versions 6.0 or later for details on using 802.1p and DiffServ.

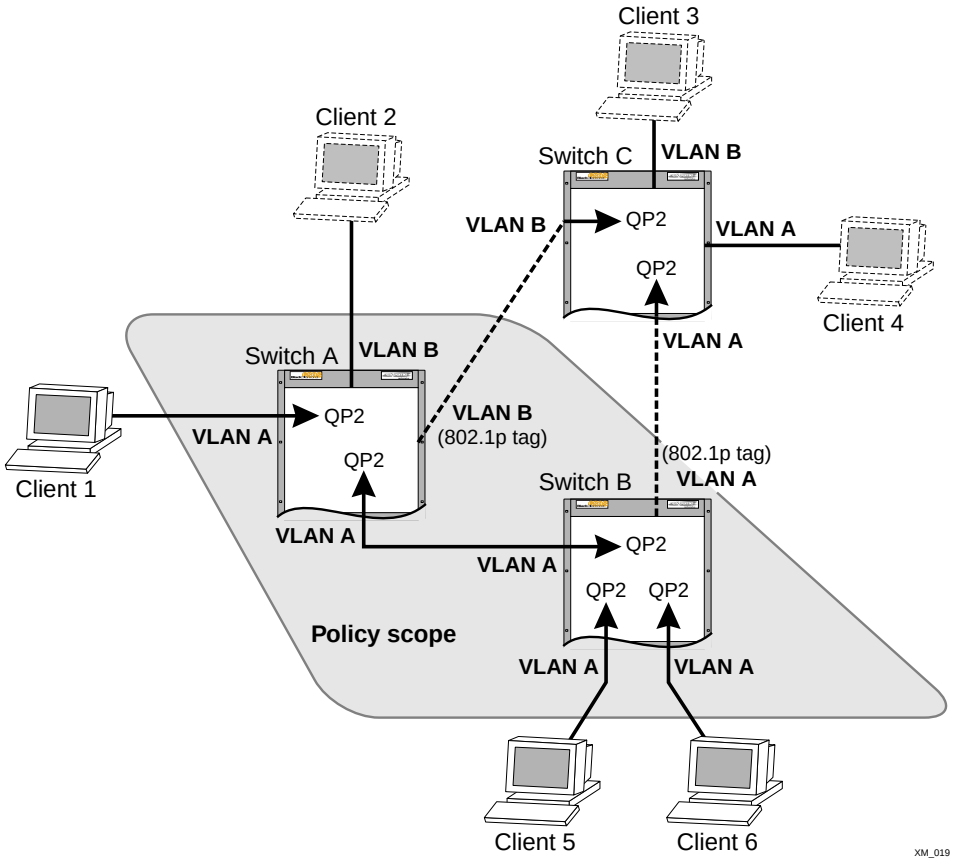
Source port QoS policies are supported on Extreme devices running ExtremeWare 5.0 or later— all *i*-series devices, and non-*i*-series devices running ExtremeWare 5.0. This means that the endpoints used to define Source Port policies must be on devices running ExtremeWare 5.0 or later.

VLAN Policies

A VLAN policy identifies traffic originating from the member ports of one or more VLANs, and assigns that traffic to a QoS profile. The Policy System implements VLAN QoS for all the traffic flows from the specified VLANs, on the devices you have defined in your policy scope.

Figure 70 shows the effects of a VLAN Policy that has been specified for VLAN A, and scoped on switches A and B. The policy specifies that traffic originating from ports that are members of VLAN A should use QoS profile QP2. Thus, this policy affects traffic originating from the ports associated with client 1 on switch A, clients 5 and 6 on switch B, and the link between switches A and B. Traffic originating from client 2 on switch A is not affected, since it originates on a port that is not a member of VLAN A. In addition, traffic originating from client 4 on switch C is also not affected, even though it is a member of VLAN A, because switch C was not included in the policy scope.

Figure 70: VLAN policy



Like Source Port QoS, VLAN QoS rules are implemented only in the devices included in the policy scope that have the specified VLAN. To enforce QoS settings across switch/VLAN boundaries you must use 802.1Q tagging—specifically through explicit packet marking using 802.1p or DiffServ. If the switch ports used for output use 802.1Q tagging, the QoS profile assignment will be carried via the 802.1p priority bits to the next switch. On *i*-series chipset devices, you can also enable DiffServ examination and replacement to observe and carry the QoS setting with the packet between switches. The use of 802.1p priority bits is enabled when you enable VLAN tagging, which you can do through the EPICenter VLAN Manager applet. DiffServ examination must be enabled using the ExtremeWare CLI or through ExtremeWare Vista. See the *ExtremeWare Software User Guide* for versions 6.0 or later for details on using 802.1p and DiffServ.

In the example shown in Figure 70, if the links between switches A and C and switches B and C use tagging (as shown in the diagram), the QoS profile information specified by the VLAN policy will be propagated into switch C, for traffic originating on the links between the switches. The tag carries information on which QoS profile should be associated with the traffic flow; the configuration of the profile itself is determined by the configuration of each individual switch.

If you want to ensure that VLAN QoS is effective end-to-end, you should make sure your switch-to-switch links use tagged ports.

Policy Named Components

The EPICenter Policy System lets you work with high-level, named components when defining a QoS policy. These high-level policy named components are mapped to policy primitive components that are actually used to create QoS rules that can be implemented in a network device.

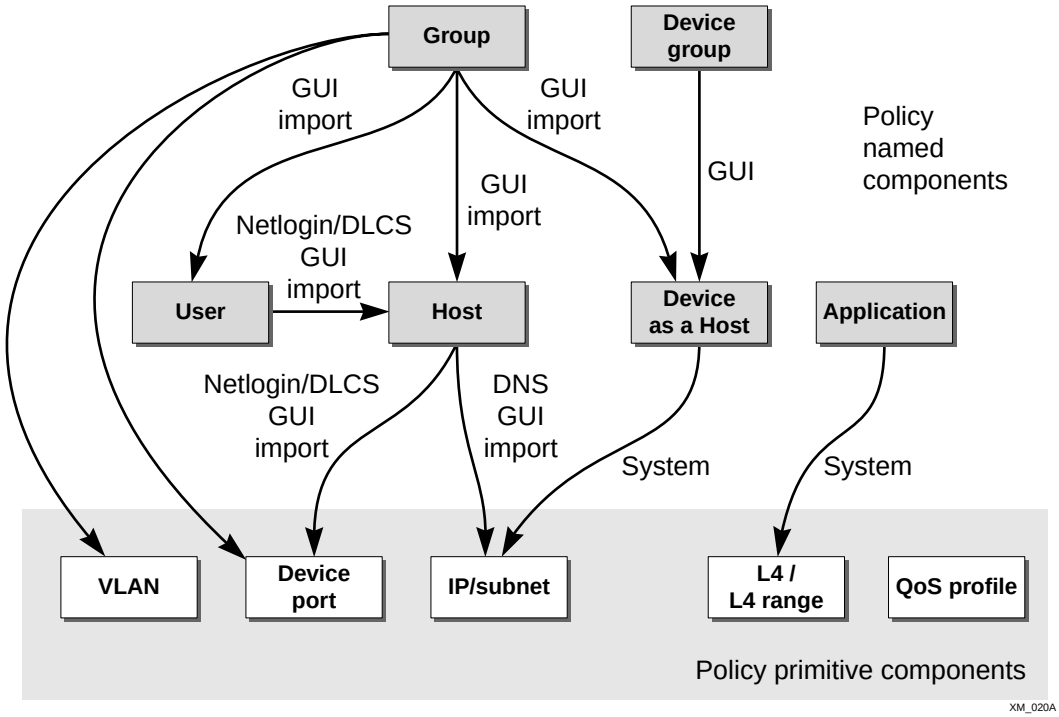
Policy named components are components such as groups (which are mapped to their individual members), users, and named hosts, which can be mapped to IP addresses and ports. These are represented by the shaded boxes in Figure 71.

Policy primitive components are components such as device ports, IP addresses, VLANs, and QoS profiles, that are used to define the QoS rules that will be implemented on a device. These are represented by the white boxes in Figure 71.

Policy named components, and most primitive policy components must be defined before they can be used in a policy definition. VLAN, device and port policy primitives must exist in the EPICenter database (that is be known to the Inventory Manager and VLAN Manager) before they can be used in a policy definition. Users, hosts, and group resources must be created (or imported) in the Grouping Manager.

IP addresses, subnets addresses, and layer 4 ports can be predefined, or can be entered directly into a policy definition through the Policy Manager user interface. In the case of Access-based Security policies, the destination port is dynamically determined.

Figure 71: EPICenter Policy Manager components



The following components are used within the EPICenter Policy Manager:

- **Groups:** Group resources (except for Device Groups) are created in the Grouping Manager. A group can contain devices, ports, custom applications, VLANs, users, hosts, as well as other groups as members. When you use a group in a policy definition, such as to define a traffic endpoint, the Policy Manager looks through the group and its subgroups, and uses in the policy definition only the resources of types that are valid for the policy you are creating.
- **Devices** (by name): Devices are entered into the EPICenter database through the Inventory Manager (Discovery or Add Devices), or the DevCLI utility, and are mapped to IP addresses in the EPICenter database. Devices are assigned to Device Groups in the Inventory Manger. They can also be added as members to other groups through the Grouping Manager.
- **Device Groups**: Device Groups are created within the Inventory Manager, and devices are assigned as members through that same applet. All devices are members of a device group. Device groups can themselves be added as members of other groups, through the Grouping Manager.
- **Hosts** (by name): Host are entered into the EPICenter database through the Grouping Manager, either using the Import capability or through the GUI. A Host to IP address mapping can be established in several ways. The IP address can be added as a component attribute through the GUI or as part of the Import function. Alternatively, the mapping can be obtained through a name lookup service such as DNS. Within the Policy server, IP addresses are mapped to physical ports on an Extreme switch using DLCS, or through relationships created in the Grouping Manager. Hosts can be added as members of groups through the Grouping Manager.
- **Applications**: Applications are named components (such as Baan, FTP, HTTP) that map to a layer 4 protocol and port. A set of applications (with protocol and port mappings) are predefined in the EPICenter database. You can also import application definitions through the Grouping Manager Import function. These definitions appear only in the Policy Manager for an IP QoS policy.
- **Custom Applications:** These are user defined applications and consist of collections of L4 ports. A custom application can consist of a mixture of UDP and TCP ports in any combination of single

ports or ranges of ports. Custom Applications are entered into the EPICenter database using the Grouping Manager.

- **Users** (by name): These are entered into the EPICenter database through the Grouping Manager, either using the Import capability or through the GUI. An individual User is typically mapped to a Host by establishing a relationship within the Grouping Manager. User-Host relationships can be specified through the Grouping Manager GUI or as part of the Import function. The Host is then in turn mapped to an IP address and physical ports as described above. Users can be added as members to groups through the Grouping Manager. For Security policies, user-host relationships are established during netlogin/802.1x login and removed upon user logout.
- **Ports**: Ports are entered into the EPICenter database through the Inventory Manager through the Discovery or Add Devices functions. They can be specified individually as part of a policy traffic definition, or they can be members of a group. Ports are added to groups through the Grouping Manager.
- **VLANs**: VLANs are detected by the Discovery or Add Device functions in the Inventory Manager, and can also be created and modified using the EPICenter VLAN Manager. They can be specified individually as part of a VLAN QoS policy traffic definition or they can be members of a group. VLANs are added to groups through the Grouping Manager.
- **IP addresses/Subnets**: IP addresses or subnet addresses are used in Security and IP QoS rules to identify IP traffic flows. IP and subnet addresses can be determined by the Policy Manager from mappings associated with named components such as users or hosts. They can also be entered directly as endpoints in an IP policy traffic definition.
- **QoS Profiles**: QoS profiles provide the definitions of traffic priority, and minimum and maximum bandwidth that, when combined with a traffic flow specification, define a policy. QoS profiles are predefined, but they can be reconfigured from within the Policy Manager.

The arrows shown in Figure 71 indicate the mapping relationships between policy named components and policy primitive components. The higher-level component at the start of the arrow can be mapped by the Policy Manager to the component at the end of the arrow. Named components may map directly to a primitive component, or they may map to another named component that in turn maps to a primitive component. For example, the Policy Manager maps a Host component directly to an IP address and a port. However, a User component specified as a traffic endpoint is mapped first to a Host, and then to an IP address and port, which is used to create the policy rules that affect traffic from that user.

The labels associated with the arrows depicts how the mapping relationship is created:

- GUI indicates that the mapping may be created through the Grouping Manager user interface.
- Netlogin/DLCS indicates that the mapping may be obtained through Netlogin or the Dynamic Link Context System (DLCS) operating within Extreme Networks devices.
- DNS indicates that the mapping may be obtained via a name lookup service such as DNS.
- IMPORT indicates that the mapping relationship can be specified during the import process in the EPICenter Grouping Manager.
- SYSTEM indicates that the mapping is predefined, or is set up by the EPICenter server, such as through the Discovery feature in the Inventory Manager.

Policy Access Domain and Scope

The policy type and policy traffic definitions specify *how* to identify a traffic flow of interest. The policy access domain (Security policy) or scope (IP policy) definition specifies how to handle that traffic flow on your network devices. The policy access domain or scope definition has three functions: It specifies the network devices on which the policy should be implemented, what the treatment should be on each device in the domain or scope.

- You can specify the domain or scope by selecting individual devices, or you can specify groups to include in the policy domain or scope.
- You specify the QoS profile that will be associated with the policy traffic for each *resource* in the domain or scope. If you specify a device individually, then you can also specify a QoS profile for that individual device. However, if you specify a group as a resource, then the QoS profile you select will apply to the policy traffic on all the devices in the group. If a device is specified more than once in the domain or scope (for example, because it is a member of two different groups that are both included in the domain), you can specify which QoS setting will take precedence.
- You specify the times of validity using the scheduler tool associated with each policy. You can select which days the policy will be active and you can specify start times and durations for each policy.

The following example illustrates some of the issues related to setting the scope for an IP policy. Since the domain for Security policies is limited to the edge device to which the user is connected, many of these issues are not relevant for Security policies.

Assume that you want to define an IP policy (Access List rule) applying to all TCP traffic (in both directions) between Host1 and Host2. This defines two traffic flows for the policy:

- From any L4 port on Host1 to any L4 port on Host2
- From any L4 port on Host2 to any L4 port on Host1

Initially, you decide to define the scope as follows:

- Include all the devices on your network (switches A, B, and C) in the scope
- Set QP1 as the profile to be used on all three devices

This means that any time any of these switches detects TCP traffic with Host1 as the source and Host2 as the destination (or vice-versa), it will assign that traffic to profile QP1.

However, in your network it happens that traffic between Host1 and Host2 would never travel through switch C, so implementing this policy on that switch is not necessary. Further, on switch B, profile QP1 is being used for some very high-priority, application-server traffic, so you want to give your TCP traffic somewhat lower priority on that switch. You can accomplish this by changing the policy scope as follows:

- Include only switches A and B in your policy scope. This will leave switch C unaffected by this policy.
- Specify profile QP1 for switch A, but a different profile (for example, QP3) for switch B. On switch B, you configure profile QP3 to have the appropriate parameters to accomplish the desired traffic prioritization.

Alternatively, it might happen that the high priority traffic on switch B is *not* using QP1, so you can use QP1 on both switches for the Host1-Host2 traffic. However, you may need to set the parameters for QP1 on switch B differently from the parameters of QP1 on switch A, to accomplish the desired traffic priorities on switch B.

It is very important to understand the relationship of the target traffic flow, the QoS profile, and the profile configuration in each switch. The policy rules generated by the EPICenter Policy Manager associate a QoS profile with a particular traffic flow, but the configuration of that profile (its bandwidth and priority parameters) are defined in each individual switch. Therefore, you may create a policy that always associates profile QP1 with the traffic between Host1 and Host2, but the actual treatment of that traffic, in terms of the minimum and maximum bandwidth and traffic priority, may be different in each switch because profile QP1 is configured differently in each switch.

Using Groups in Policy Definitions

In many cases, you may want to define multiple policies that should apply to the same set of endpoints, or that should have the same set of devices as the policy domain or scope. The ability to create groups of users, hosts, devices, ports, custom applications, and VLANs can make the definition of these policies easier.

For example, you may want to define several Access List policies to prioritize traffic between several different application servers and a specific set of users. To accomplish this easily, you could create a group that contains those users, and then use the group as the user or client endpoint in the traffic definition for each of the policies you create. Further, you may want to include the same set of network devices in the scope for these policies. Again, you can create a group for these devices, and use that group to define the scope for each of the policies.

You can use the Grouping Manager to define a group of users:

- Use the EPICenter Grouping Manager to define the user resources, either by entering them individually through the GUI or by importing them.
- Ensure that a mapping relationship exists from each user to an IP address. This is necessary so that the Policy Manager can use them to create identifiable traffic flows. User-host-IP address relationships are often created as part of the import process. If Netlogin/DLCS is running on your Extreme network devices, it may do this mapping for you. You can also create these relationships directly through the Grouping Manager GUI. In the case of Access-based access-based Security policies, the user IP is dynamically determined when the user logs into the system
- When you have your user resources set up and mapped to IP addresses, you can create a group and add your users as members of the group.

To create a group for the devices you want to use for the policy scope, you have two options:

- You can create a Device Group in the Inventory Manager, and assign the devices to this group.
- You can add devices as members of a non-exclusive resource group through the Grouping Manager. The same device can be a member of multiple groups of this type, so future grouping requirements do not need to impact the group you set up for your policy scope purpose.

Regardless of how you set up your group, you can then use this group to specify the scope for the policies you create.

There is one consideration in using a group of devices in a policy scope, which is that the same QoS profile applies to the entire group. For example, if you specify a group in the policy scope, and assign profile QP3 to that group, all devices included in the group will then use QP3 for that policy. The configuration of QP3 may be different on each device, but the policy will always apply QP3, however it is defined, to the traffic flow defined by the policy. (The Policy Manager does allow you to inspect the QoS profiles and their association with policies on devices or device ports, and you can adjust the settings if needed).

The Grouping Manager allows groups to contain members of different resource types, including other groups. However, when you are setting up groups for use with the Policy Manager, it is recommended that you create relatively simple groups that contain only the resources that you intend to use for a single purpose.

For example, when you use a group to define a traffic flow, you are specifying that all members of that group (that can be mapped to an IP address) are endpoints of the specified traffic flow. If you define a large group that is used for a variety of purposes, especially one with subgroups as members, you need to ensure that it does not contain members that will result in policy traffic flows other than the ones you intended to specify.

Furthermore, if the membership of the group changes after you have implemented your policies, the endpoints for the traffic flow will change. If you have policy auto-configuration enabled, new policy rules will automatically be computed and configured on your network, based on the new traffic flow definition.

Precedence Relationships within the Policy Manager

The EPICenter Policy Manager has several types of precedence relationships:

- Precedence between resources within the scope of a policy
- Precedence between EPICenter policies
- Precedence between the QoS rules implemented on an Extreme Networks device

Each of these has a somewhat different use and effect.

Precedence between the resources in a policy scope is used to determine which QoS profile specification should be used when a particular device is specified multiple times within a scope definition.

Policy precedence (precedence between policies) is used to determine which policy should be used when multiple policies could apply to the same traffic flow. If this occurs, the policy with higher priority is used by the switch over policies of lower priority. Policy precedence only controls the relationships between policies of the same type. Policies of different types have a predefined precedence relationship: IP QoS policies are the highest priority, Source Port QoS policies are second, and VLAN QoS policies have the lowest priority.

For IP policies, policy precedence is implemented by assigning precedence numbers to IP access-lists that are configured to the devices. These precedence numbers may be different on different devices depending on how many policies are active on a given device. The actual IP access-list precedence number is not as important because it is the relative ordering between the precedence numbers from the access-list that matters.

Policy Configuration

The EPICenter Policy Manager supports automatic configuration of QoS policies. If Auto Configuration is enabled, every change you make on a device or within the EPICenter software has the potential to trigger an immediate recomputation and reconfiguration of the QoS policies on your network. An automatic reconfiguration can be triggered by any of the following events:

- Changes to group memberships made through the Grouping Manager or Inventory Manager that affect a group used to define a policy endpoint or policy scope

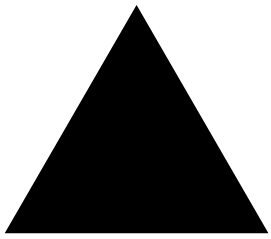
- Changes made through the ExtremeWare CLI or ExtremeWare Vista on a device managed by the EPICenter server
- A user login or end station reboot when DLCS is enabled
- Saving a change to a policy within the Policy Manager

If Auto Configuration is disabled, you must explicitly perform the configuration process using one of the directed configuration functions initiated using the **Configure** or **Configure All** buttons on the Policy Manager toolbar.

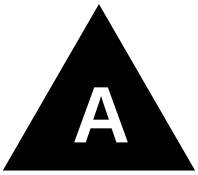
The EPICenter policy server also supports policy enabling and disabling, and policy configuration through an external access protocol and API. External applications can use Tcl functions to enable and disable policies, and to configure policies on specified devices. The external access protocol and Client Tcl API are documented in Appendix E of this manual.

EPICenter Policy Limitations

The EPICenter Policy Manager does not support the entire set of policy-based QoS features found in the most current versions of the ExtremeWare software. In addition, not all versions of the ExtremeWare software support all the features available through the Policy Manager.



Appendices



Troubleshooting

This appendix describes how to:

- Resolve problems you may encounter that are related to the EPICenter server
- Resolve problems you may encounter while using the EPICenter client application

Troubleshooting Aids

If you are having problems with EPICenter, there are several things you can do to help prevent or diagnose problems.

Using the Stand-alone Client Application

To enable debugging and log the output to a file in the stand-alone client application, you can run the EPICenter client in debug mode.

In Windows 2000/XP, enter one of the following commands at the prompt in a command window or in the **Run** field.

If you have both server and client installed on the same system:

```
c:\Program Files\Extreme Networks\EPICenter 5.0 > runclient.exe DEBUG DEBUG >
<logfile>
```

If you have the client only installed:

```
c:\Program Files\Extreme Networks\EPICenter 5.0 > runclient.exe DEBUG DEBUG >
<logfile>
```

In Solaris, enter the one of the following commands at a command prompt.

If you have both server and client installed on the same system:

```
/opt/extreme/epc5_0/runclient DEBUG DEBUG >& <logfile>
```

If you have the client only installed:

```
/opt/extreme/epc5_0_client/runclient DEBUG DEBUG >& <logfile>
```

<*logfile*> is the name of the log file to be created. If you installed the client on a different drive and directory, make the appropriate substitutions. Optionally, piping output to "tee," if you have it available, allows you to see the logs on the console as well as logging the data into the file.

Be sure to use different log file names if you are running multiple clients on the same machine.

Using the Browser-based Client (Windows Only)

NOTE

After a problem occurs, prior to pointing the browser to the EPICenter server, it is recommended that you clear all browser cache information, including disk cache, and close and re-open the browser.

If you are using the browser-based client, please try to duplicate the problem with the Java Console enabled in Internet Explorer. Look at the Java Console window and copy/paste (using [Ctrl]+C and [Ctrl]+V on Windows 2000/XP) the contents into a text file. If a problem occurs, Extreme Networks customer support may require the Java Console output.

In addition, you can run the client in a debug mode in the browser:

1. Start the client with the URL http://<host>:<port>/everest/debug.
2. After you enter your login information, but before the main EPICenter page is displayed, a page with debug settings is displayed.
3. Select **Info** for "Client Debug Level."
4. Click **Submit Query**.

This enables more detailed information to be logged.

Enable the Java Console

To facilitate problem diagnosis, you can attempt to duplicate the problem with the Java Console enabled. To enable the Java Console, do the following:

1. From the Windows **Start** menu, select **Programs**, then **Java Plug-in Control Panel** and launch the Control Panel.
2. On the **Basic** page, click the **Show Java Console** check box.
3. Click **Apply.**

The next time you launch the EPICenter client, the Java Console will start automatically.

NOTE

Running with the Java Console displayed may reduce the performance of the EPICenter client.

There is limited space for Java Console messages; once the console log file is filled, no more messages will be recorded. If you are trying to duplicate a problem, clear the Java Console log file periodically by clicking the **Clear** button at the bottom of the window.

You can close the Java Console by clicking the **Close** button at the bottom of the window. However, once it is closed, it can only be restarted by closing and restarting the browser.

EPICenter Client

Problem: Client is unable to connect to the EPICenter server.

Verify that the EPICenter Server process is running.

Verify that the server is running on the specified port. You can try to connect to the server's HTTP port using a browser. If the server is running and you are using the correct port, the EPICenter main page will be displayed.

If you are running the client on the same system as the EPICenter server, you can also use the Port Configuration utility to determine the port on which the EPICenter server is running.

To run the Port Configuration utility, go to the Windows **Start** menu, and select **Programs**, then **Extreme Networks**, followed by **EPICenter 5.0**, then **Port Configuration**.

For more information on the Port Configuration utility, see Appendix B.

Problem: Colors in client interface are incorrect (Windows 2000, Windows XP).

The Color Palette must be set for 65536 colors (or True Color). If your display is set for only 256 colors, the colors in the left-hand panel (the Navigation Toolbar) and the EPICenter applets themselves may be incorrect.

To change the color palette, double-click the **Display** icon in the **Control Panel**, select the **Settings** tab, and use the drop-down list in the **Color Palette** field to select the appropriate setting.

Problem: After running for a while, the display disappears in some applets (Windows, browser only).

Under some conditions in the browser client, the Java Plug-in can run out of memory. If you are running with the Java Console enabled, you may see "Out of Memory" errors recorded in the console log file. To alleviate this problem, you can grant the plug-in more memory through the Java Plug-in Control Panel.

1 From the Windows **Start** menu, run the **Java Plug-in Control Panel**.

  The Plug-in Control Panel should appear with the **Basic** page displayed.

2 In the Java RunTime Parameters field, enter the following without any embedded spaces:

  `-Xmx`*`nnn`*`m`

  nnn is the maximum number of megabytes of virtual memory available to the plug-in.

  For example, entering **`-Xmx128m`** allows the plug-in to use up to 128 MBytes of virtual memory, and should prevent out-of-memory problem.

3 If you see similar problems with the client application, restart the client to fix the problem.

Problem: Browser does not bring up the Login page.

Verify the version of the browser you are using. See the system requirements in Chapter 1 or see the *EPICenter Release Note* shipped with the software.

Problem: Browser client software loads and allows login, but data is missing or other problems arise.

Clear your browser's cache, exit the browser, and restart it. This frequently clears up miscellaneous start-up problems in the client.

In Internet Explorer, clear cache by selecting **Internet Options** under the **Tools** Menu, then clicking **Delete Files** under the Temporary Internet Files section of the **General** tab.

Problem: Cannot cut, paste or print from the browser-based client, or save to the local file system.

As of EPICenter 4.0 the browser-based client no longer supports cut/paste/print or save from the browser-based client. These functions are supported only in the stand-alone client application.

EPICenter Database

Problem: DBBACKUP utility will not run if LD_LIBRARY_PATH variable is not set correctly

In order for DBBACKUP to run, the LD_LIBRARY_PATH environment variable must include the path `<install_dir>/database` (by default, `/opt/epc_30/database`). There are some needed `.so` files in that directory. (10051)

Problem: Database server will not restart after incorrect shut down

If the EPICenter server is shut down incorrectly, the database may be left in an invalid state. In this case, an "Assertion failed" error may occur when attempting to restart the server.

To recover the database in Windows 2000 or Windows XP, do the following:

1. Open a DOS command window.

   The following commands assume you have accepted the default installation location, `c:\Program Files\Extreme Networks\EPICenter 5.0`. If you have installed EPICenter in a different location, substitute the correct installation directory in the commands below.

2. Go to the EPICenter install directory:

   ```
   cd c:\Program Files\Extreme Networks\EPICenter 5.0
   ```

3. Add the EPICenter database directory to your path:

   ```
   set path=c:\Program Files\Extreme Networks\EPICenter 5.0\database;%path%
   ```

4. Execute the following command:

   ```
   database\dbeng9.exe -f basecamp.db
   ```

5. Watch the output from this command. If the database program indicates it cannot recover the database, delete the database log:

   ```
   del basecamp.log
   ```

   and try executing the previous command again:

   ```
   database\dbeng9.exe -f basecamp.db
   ```

6. If the database is successfully recovered, restart the server.

   If the database cannot be recovered, you will need to restore the database from a backup. See Appendix C in the *EPICenter Reference Guide* for instructions on restoring the database from a backup.

To recover the database in Solaris, do the following:

1. Open a shell window (csh is used for the following example).

   The following commands assume you have accepted the default installation location, `/opt/extreme/epc5_0`. If you have installed EPICenter in a different location, substitute the correct installation directory in the commands below.

2 Go to the EPICenter install directory:

```
cd /opt/extreme/epc5_0
```

3 Make sure the `LD_LIBRARY_PATH` environment variable is set to the EPICenter directory installation directory:

```
setenv LD_LIBRARY_PATH /opt/extreme/epc5_0/database
```

4 Execute the following command:

```
database/dbeng9.exe -f basecamp.db
```

5 Watch the output from this command. If the database program indicates it cannot recover the database, delete the database log:

```
rm basecamp.log
```

and try executing the previous command again:

```
database/dbeng9.exe -f basecamp.db
```

6 If the database is successfully recovered, restart the server.

If the database cannot be recovered, you will need to restore the database from a backup. See Appendix C in the *EPICenter Reference Guide* for instructions on restoring the database from a backup.

EPICenter Server Issues

Problem: Cannot talk to a specific switch.

Verify that the switch is running ExtremeWare software version 2.0 or later.

Ping the switch's IP address to verify availability of a route. Use the **`ping`** command from a MS DOS or Solaris command shell.

If the switch is using SNMPv1, verify that the read and write community strings used in EPICenter match those configured on the switch. If the switch is using SNMPv3, verify that the SNMPv3 parameters configured in EPICenter match those on the switch.

Problem: ExtremeWare CLI or ExtremeWare Vista changes are not reflected in EPICenter.

Verify that the switch is running ExtremeWare software version 2.0 or later.

From the Inventory Manager, click **Sync** to update the information from the switch. This refreshes the switch specific data, validates the SmartTrap rules, and ensures that the EPICenter server is added as a trap receiver (Extreme switches only).

If the problem persists, verify that the EPICenter workstation has been added in the list of trap destinations on the given switch:

1 Telnet to the switch.

2 Log in to the switch.

3 Type **`show management`** to verify that the system running the EPICenter is a trap receiver, or **`show snmpv3 target-addr <ipaddress>`** if the device is running SNMPv3.

An Extreme switch can support a maximum of 6 trap destinations in ExtremeWare 2.0, and up to 16 trap destinations with ExtremeWare 5.0 or greater. If EPICenter is not specified as a trap destination, then no

SmartTraps are sent, and the data is not refreshed. If you need to remove a trap receiver from a device running SNMPv1, use the command:

```
config snmp delete trapreceiver <ipaddress>
```

For devices running SNMPv3, use the commands:

```
config snmpv3 delete target-addr <ipaddress>
config snmpv3 delete target-params [ <param> | all ]
config snmpv3 delete notify [ <notify-name> | all-non-defaults ]
```

See the *ExtremeWare Software User Guide* for information on using these commands. These commands will also delete SNMPv1 trap receivers.

For convenience you may want to create a Telnet macro containing these commands. You can use a user-defined variable to input the target IP address.

Problem: Need to change SNMP polling interval, SNMP request time-out, or number of SNMP request retries.

You can change the default values for the SNMP polling interval, the SNMP request time-out, or the number of SNMP request retries, through the Administration applet, Server Properties page.

See Chapter 15 in the *EPICenter Reference Guide* for information on the EPICenter Administration applet.

Problem: Need to change the Telnet or HTTP port numbers used to communicate with managed devices.

You can change the port numbers for all managed switches through the Administration applet, Server Properties page.

See Chapter 15 in the *EPICenter Reference Guide* for information on the EPICenter Administration applet.

Problem: Telnet polling messages can fill up a device's syslog file.

For switches running older versions of ExtremeWare (prior to 6.0), the EPICenter server uses Telnet polling to get EDP topology and ESRP information. EPICenter also uses telnet polling to get Netlogin information, Alpine power supply IDs, and for doing MAC Address polling. However, each Telnet login and logout message is logged to the switch's log file, and will eventually fill up the log.

You can disable Telnet polling through the EPICenter Administration applet to avoid the messages to the switch log file. However, this disable all Telnet polling, including the MAC Address Poller used for edge port polling. If Telnet polling is enabled, you can then enable and disable MAC Address polling separately through the MAC Polling Server Properties in the Administration applet. You can also enable and disable MAC Address polling for individual switches through the Inventory Manager.

See Chapter 15 in the *EPICenter Reference Guide* for information on the EPICenter Administration applet.

Problem: Traps may be dropped during a trap "storm."

The EPICenter server limits its processing of traps in order to be able to reliably handle trap storms from a single or multiple devices. EPICenter limits its trap processing to 20 traps every 28 seconds from an individual device, and a total of 275 traps every 55 seconds system-wide. Any traps that occur beyond these limits will be discarded, but will be noted in the `log.txt` file.

Exceeding the first limit (>20 traps in 28 seconds) is rare, and should be considered abnormal behavior in the managed device. If you are managing a large number of devices, you may reach the total (275) limit in normal circumstances. If you are managing more than 1000 devices, it is recommended that you increase the total number of traps to 500.

The trap processing limits can be changed through server properties in the Administration applet. See Chapter 15 in the *EPICenter Reference Guide* for more information on setting EPICenter server properties.

Problem: Under Solaris, an error occurs when attempting to enable the EPICenter Syslog server function.

By default, Solaris runs its own Syslog server. This causes an error "Syslog Server unable to start: Address already in use" when you attempt to enable the EPICenter syslog server. You must first stop the Solaris syslog server in order to have EPICenter act as a Syslog receiver. To stop the Solaris Syslog server, use the command:

```
/etc/init.d/syslog stop
```

Problem: EPICenter is not receiving traps.

If the IP address of an EPICenter host is changed via DHCP while EPICenter is running, the system will not receive traps. To fix the problem, you can do a manual sync on all devices, or restart the EPICenter server.

Problem: On a Windows system with multiple NICs, EPICenter may not receive traps or be able to upload or download configuration files or images.

In Windows, in a multiple NIC cards environment, the IP address that EPICenter gets as the primary IP address is determined by the order in which the network connection is listed in the 'Adapters and Bindings' tab in Advanced Settings, and may not be the NIC that is actually connected to the management network. There is no guarantee that the primary IP address that gets registered as a trap receiver on a switch is the IP address of the NIC that EPICenter actually uses to communicate.

You may be able to work around this by changing the order of the IP addresses in the Adapters and Bindings tab in the select the primary IP address for EPICenter to use:

1. From the **Start** menu select **Settings**, then select **Network and Dial-up Connections**. You can also open the Network and Dial-up Connections window from the control Panel.
2. From the **Advanced menu**, select **Advanced Settings...**
3. Select the **Adapters and Bindings** tab, which shows the connections listed in order.
4. Select the connection you want EPICenter to use, use the up and down arrow buttons at the right to move it to the top of the list, then click **OK**
5. Restart the EPICenter server.

Problem: Policy Manager button does not appear in the Navigation Toolbar.

The EPICenter Policy Manager is a separately licensed module, and requires installation of a separate license key through the `instlic` license key utility. When you purchase the right to use the Policy Manager applet, you will receive an activation key, found on the License Agreement included in your software package. This key starts with "AC," and can be used to obtain a permanent license key. You do not need an activation key to obtain an evaluation license key.

To obtain a license key, use your browser to connect to the license page at http://www.extremenetworks.com/go/epickey.htm. You can obtain an evaluation key or a permanent key through this page. You will need your activation key to obtain a permanent license key. In either case, you

will be asked to enter some information about yourself, and the license key will be sent to you by return e-mail. Follow the instructions in the *EPICenter Installation and Upgrade Note* or the *EPICenter Release Notes* to add this license to your EPICenter installation.

VLAN Manager

Problem: Multiple VLANs have the same name.

A VLAN is defined by the name, its tag value, and its protocol filter definition. EPICenter allows multiple VLANs of the same name if one of the defining characteristics of one VLAN is different from the other.

Problem: Multiple protocols have the same name.

EPICenter allows multiple protocols of the same name if one of the defining characteristics of one protocol is different from the other.

Problem: Created a new protocol in VLAN Manager, but the protocol does not appear on any switch.

When a new protocol is created, it is stored in the EPICenter database. EPICenter only creates the protocol on a switch when the new protocol is used by a VLAN on that switch.

Problem: Can only access one of the IP addresses on a VLAN configured with a secondary IP address.

EPICenter does not currently support secondary IP addressing for a VLAN.

Problem: Configuration fails when attempting to configure a VLAN with a modified protocol definition.

EPICenter does not have a mechanism to modify protocols. When a VLAN is configured through EPICenter to use a protocol that does not exist on the switch, the protocol is first created on the switch. However, if a protocol with the same name but a different definition already exists on the switch, the operation will fail.

Problem: An untagged port has disappeared from its VLAN.

Check to see if the port has been added as an untagged port to a different VLAN. In EPICenter, adding an untagged port to a VLAN automatically removes the port from its previous VLAN if the port was untagged, and the new and old VLANs used the same protocol. You should receive a warning message when this happens, which lets you proceed with the auto-deletion or cancel the operation. This is different behavior from the ExtremeWare CLI, where you must first delete the port from the old VLAN before you can add it to the new VLAN.

Problem: When you delete a VLAN, the VLAN remains in the VLAN tree, but with no members

EPICenter does not immediately clean up the VLAN tree. It can take up to 24 hours before the VLAN will disappear from the tree.

Alarm System

Problem: Device is in a fault state that should generate a trap or syslog message, and an alarm is defined to detect it, but the alarm does not appear in the EPICenter Alarm Log.

There are several possible reasons this can occur. Check the following:

- Make sure that the alarm is defined and enabled.
- Check that the device is in your alarm scope.
- Check that SNMP traps are enabled on the device.
- For a non-Extreme Networks device, make sure you have set EPICenter as a trap receiver on the device (see Chapter 8).
- For an RMON alarm, make sure you have RMON enabled on the device.
- For Syslog messages, make sure that you have the EPICenter Syslog server enabled, and that remote logging is enabled on the device with EPICenter set as a Syslog receiver.
- The number of traps being received by the EPICenter server may exceed the number of traps it can handle in a given time period, resulting in some traps being dropped (see the item on dropping traps on page 170). You can change the limits for the number of traps the server should accept (per minute and per 1/2 minute) in the Administration applet. See Chapter 15 in the *EPICenter Reference Guide* for more information on setting EPICenter server properties.

Problem: The "Email to:" and "Short email to:" fields are greyed-out in the Actions tab of the New Alarm Definition dialog.

You need to specify an e-mail server in order to send e-mail. Click the **Settings...** button next to the **Email to** field to set up your mail server.

Problem: An RMON rule is defined to monitor a counter variable, and to cause an alarm when the counter exceeds a certain value. The counter has exceeded the threshold value but no alarm has occurred.

There are several things to check:

- Make sure the RMON rule and the alarm definition are set up correctly
- If the value of the counter was already above the threshold value when you set up the RMON rule, and you have the Sample Type set to Absolute, no alarm will ever be generated. This because the value must fall below the Falling Threshold value before the before another Rising Threshold trap will be sent, and this will never occur. You should consider using the Delta Sample Type instead.

Problem: When creating an RMON rule in the RMON Rule Configuration window, the MIB variable I want to use is missing from the list of variables displayed when I click "Lookup..."

The MIB Variable list displays only the MIBs shipped with the EPICenter software. In addition, within those MIBs the variable list will not display variables that are indexed by an index other than (or in addition to) ifIndex. You can still use variables that do not appear in the Lookup... list, but you must type the complete OID into the MIB Variable field, in numeric notation. If the variable is a table variable, you will need to append the specific index and apply the variable to each target device, one at a time.

Problem: A program specified as an action for an alarm (in the Run Program field) does not get executed. It includes output to the desktop among its functions.

If you are running the EPICenter server as a service, you must specifically tell it to allow output to the desktop. To do this you must stop and restart the EPICenter server, as follows:

1. In the Services properties window, select **EPICenter 5.0 Server** and click **Stop**. (To find the Services window, from the Start menu select Settings, then Control Panel, the double-click the Services icon).
2. When the **EPICenter 5.0 Server** service has be stopped, select it again and click **Startup...**. This displays a pop-up window where you can specify start-up options.
3. In the lower part of the window, in the **Log On As:** area, click the box labeled **Allow Service to Interact with Desktop**. Then click **OK**.

After the EPICenter server restarts, the program you have specified as an alarm action should execute correctly.

To specify a batch file that does output to the desktop, you must specify the ".bat" file within a DOS "cmd" command, as follows:

```
cmd /c start <file.bat>
```

where <*file.bat*> is the batch file you want to run.

Problem: Email alarm actions generate too much text for a text pager.

You can use the "Short email to:" option to send an abbreviated message appropriate for a text pager or cell phone. The short email provides only very basic alarm information. See Chapter 9 for more details on using the email options as an alarm action.

Problem: Alarm action that executes a script does not run to completion.

Check to determine if a command in the script has failed. If one command in the script fails, the rest of the script will not be executed. This is expected behavior.

If you want to execute multiple script commands regardless of individual command failure, you must catch the exception thrown in each command. For example, a script action:

```
catch {do Command1}
catch {do Command2}
```

will execute Command2 even if command1 fails. For detailed information on how to use the Tcl script, consult the Tcl man pages or Help file at http://www.tcl.tk.

ESRP Monitor

Problem: None of the member VLANs of an ESRP group are appearing in the ESRP Manager applet.

Make sure that all members of the ESRP group use the same election algorithm. If there is an election algorithm mismatch between any of the ESRP-enabled switches in any of the ESRP-enabled VLANs in the ESRP group, this causes a misconfiguration scenario, and ESRP will not function. As a result, none of the members of the ESRP group will appear in the ESRP Manager applet.

Problem: Some of the switches in an ESRP-enabled VLAN are missing from the ESRP Manager applet.

Make sure that the Hello Timer (ESRP Timer) is set to the same interval for all ESRP-enabled switches. If there is a timer mismatch, ESRP will not function correctly, and the ESRP Manager applet will not be able to detect ESRP switch neighbors that are not being managed by the EPICenter software.

Problem: Devices running ExtremeWare 4.x are not being polled for ESRP information.

The EPICenter server uses Telnet polling to add and update ESRP information for devices running ExtremeWare 4.x. If you have the "Poll devices using Telnet" option disabled in the Administration applet, no ESRP information will be obtained for these devices. You can enable telnet polling through the Server Properties page in the Administration applet. See Chapter 15 in the *EPICenter Reference Guide* for more information.

Inventory Manager

Problem: Multiple switches have the same name.

This is because the sysName of those switches is the same. Typically, Extreme Networks switches are shipped with the sysName set to the type of the switch "Summit48," "Summit1i," "Alpine3808," and so on, depending on the type of switch.

You can change the way names are displayed through a sever property in the Administration applet. You can display devices in the Component Tree by name or by IP address and name. See Chapter 15 in the *EPICenter Reference Guide* for more information on setting EPICenter server properties.

Problem: Discovery does not display the MAC address for some devices in discovery results list. In addition, may not add the device to inventory (primarily happens with workstations).

If the MAC address is not found in the first instance of ifPhysAddress, it is not displayed in the discovery results table. However, when the device is selected to be added to the EPICenter inventory, the Inventory applet searches all the ifPhysAddress entries for the device, and will use the MAC address found in this manner. If no MAC address is found in any ifPhysAddress entry, the device will not be added to the EPICenter database.

Problem: Attempted to add a switch in the Inventory Manager after rebooting the switch, and received an "SNMP not responding" error.

If a switch has recently been powered on, it may take some time (a number of minutes) before the device is completely initialized. This will be especially true of chassis devices with many blades, or devices with a large number of VLANs configured on the device. It the device has not completed its initialization, the Inventory Add process may return an error. You can simply wait until the device has finished initializing and try the Add function again.

Problem: For a device selected under Status, the Device Information panel shows incorrect information, and the device image is not displayed correctly.

This can be caused by a device IP address that is in conflict with another device on the network (a duplicate IP address). Remove the problem device from the EPICenter inventory, and add it in again with the correct IP address.

Grouping Manager

Problem: Cannot import users from Windows Domain Controller

The EPICenter Server must be running with permissions that enable it to get user information from a Domain Controller. To verify and change permissions for the Web Server, do the following:

1. From the **Start** menu, highlight **Settings**, pull right, and click on the **Control Panel**. This displays the Control Panel folder.
2. Double-click on **Services** to display the Services Properties window.
3. In the Services properties window, select **EPICenter 5.0 Server** and click **Stop**. (To find the Services window, from the Start menu select Settings, then Control Panel, the double-click the Services icon).
4. When the **EPICenter 5.0 Server** service has be stopped, select it again and click **Startup...**. This displays a pop-up window where you can specify start-up options.
5. In the lower part of the window, in the **Log On As:** area, enter the account name and password for a user who has the appropriate permissions to access the Domain Controller.
6. Click **OK** to restart the Web Server service to have the new user logon take effect.

Printing

Problem: When printing a topology map from the browser client, or a printing report, the browser can appear to freeze.

Printing a report or a topology map can cause the browser utilization to become very high (approaching 100%) and can spool a very large amount of memory. There is no current solution other than to wait, and the process will eventually finish.

Topology

Problem: In Map Properties, changed the node background color, but only some of the node backgrounds changed.

The background color affects submap nodes, device hyper nodes and device or decorative nodes that do not display the device icon (either because the icon display is turned off or the nodes have been reduced in size to where the icon cannot be displayed). For device nodes and decorative nodes with the device icon displayed, the background color is transparent, and the background color setting is ignored.

Problem: A link has been moved, but the old link still appears as a down or unknown link.

When a previously “up” link disappears, the EPICenter server cannot tell if whether it is down or has been physically moved, so it changes its status to down (or unknown). EPICenter will detect the new link and add it as an up link, but it will not remove the old link.

To remove non-existent links, you can use the Sync Links command in the Topology applet. This command will remove all down links. Note that this command will also remove existing links that are down, but EPICenter will rediscover and add back those links when they come back up.

Problem: The Sync Links command removed legitimate links that were down.

The EPICenter server cannot discover a link if the link is down. Therefore, when it rediscovers links it will only discover up links (or partially up links in the case of composite links). However, down links will automatically reappear when they come up again. You can also use the Sync Links command again after the down links have come back up.

STP Monitor

Problem: There are multiple STP nodes with the same name.

The EPICenter server identifies an STP domain by its name and tag. If you see multiple STP domains in EPICenter, you may have a misconfiguration where the same STP domains are configured with different tags on different switches.

Reports

Problem: After viewing reports, added a user-defined report, but it doesn't appear in the list of reports on the main reports page.

The Reports page updates the list of reports when the page is loaded. To update the list, Refresh the page.

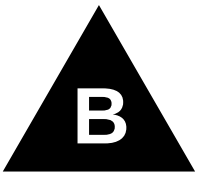
Problem: Reports cannot be launched.

Due to a problem with Windows, sometimes reports cannot be launched from the EPICenter client. To work around this problem, you can either set your browser home page to blank, or you can run the Reports feature directly from the browser:

1. Point the browser to the URL of the EPICenter server:

   `http://<host>:<port>/`

   In the URL, replace *<host>* with the name of the system where the EPICenter server is running. Replace *<port>* with the TCP port number that you assigned to the EPICenter Web Server during installation.
2. Click the **View Reports** link.
3. Login to the Reports feature.



EPICenter Utilities

This appendix describes several utilities and scripts shipped with the EPICenter software:

- The DevCLI utility, that can be used to add, modify, delete, and sync devices and device groups; and can be used to modify device configuration information from the EPICenter database using the `devcli` command
- The Inventory Export scripts, that can be used to extract information from the EPICenter inventory and output it to the console or to a file
- The SNMPCLI utility, that can be used to inspect the contents of device MIBs
- The Port Configuration utility, a Windows-only utility that you can use to change the ports used by the EPICenter server
- The AlarmMgr utility, used to display alarm information from the EPICenter database. Results can be output to a file.
- The FindAddr utility, used to find IP or MAC addresses within a set of devices or ports (specified individually or as device or port groups). Results can be output to a file.
- The TransferMgr utility, used to upload or download device configurations, or to download new software versions.
- The VlanMgr utility, used to create, reset, and delete VLANs.
- The ImportResources utility, used to import resources into the Grouping Manager from an external source such as an LDAP or Windows Domain Controller directory.

The DevCLI Utility

The DevCLI utility allows you to add, modify, and remove devices and device groups from an EPICenter database using a command line statement, rather than through the EPICenter client user interface. You can add devices and device groups individually or in groups, and you can specify arguments such as community strings and login and passwords for both the EPICenter server and the devices. You can modify device and device group settings as well as device configurations. You can specify a list of devices in a file and have them added in a single operation.

The DevCLI is useful for updating the EPICenter inventory database quickly when large numbers of devices or device groups are added, modified or removed, or if changes occur frequently. It can also be useful when you want to duplicate the device inventory and device group configurations across multiple installations of the EPICenter server.

Using the DevCLI Commands

The utility is located in the root EPICenter install directory, by default `\Program Files\Extreme Networks\EPICenter 5.0` in a Windows environment, or `/opt/extreme/epc5_0` in a Solaris environment.

The DevCLI utility supports the following four commands:

- **`devcli add`** <*`options`*> to add a device or device group.

  To add device 10.205.0.99 to the EPICenter database on the local host, using the default device user name and password, enter the following command at the prompt:
  `devcli add -u admin -a 10.205.0.99`

  To add a device group to the EPICenter database with the name "Device Group 1," enter the following command at the prompt:
  `devcli add -u admin -g "Device Group 1"`

  To add multiple device groups to the EPICenter database with the names "Device Group 1" and "Device Group 2," enter the following command at the prompt:
  `devcli add -u admin -g "Device Group 1" -g "Device Group 2" -g "Device Group 3"`

- **`devcli mod`** <*`options`*> to modify a device or device group.

  To modify the password on device 10.205.1.51 to use an empty string, enter the command :
  `devcli mod -u admin -a 10.205.1.51 -d ""`

  NOTE

  If you are running the DevCLI on a Windows platform, enter forward slashes to separate empty double quotes to ensure the command executes correctly. For example, to use the previous command in a Windows environment, enter the command: `devcli mod -u admin -a 10.205.1.51 -d \"\"`

  To modify the name of a device group from "Device Group 1" to "New Device Group," enter the following command at the prompt:
  `devcli mod -u admin -g "Device Group 1" -m "New Device Group"`

- **`devcli del`** <*`options`*> to remove a device or device group.

  To remove device 10.205.0.99 from the EPICenter database, enter the command:
  `devcli del -u admin -a 10.205.0.99`

  To remove a device group named "New Device Group" from the EPICenter database, enter the command:
  `devcli del -u admin -g "New Device Group"`

- **`devcli sync`** <*`options`*> to manually update device configurations.

  To manually update the device configurations for device 10.205.0.99, enter the command:
  `devcli sync -u admin -a 10.205.0.99`

  To manually update the configurations for the default device group, enter the command:
  `devcli sync -u admin -g Default`

  NOTE

  You can type either `sync` *or* `syn` *when you use the* `devcli sync` *command.*

These commands support a set of options for specifying device information such as passwords and community strings, device group information such as device group names and member devices, as well as information about the EPICenter server, such as host name or IP address, port, and user name and password. You can also specify multiple IP addresses in a file to have them added or removed as a group, as long as they all use the same user name, password, and community strings.

Table 6 specifies the options you can use with these commands:

Table 6: DevCLI command options

Option	Value	Default
-a	Device IP address. This option can be specified more than once.	None
-b	SNMP version 3 user name.	initialmd5
-c	Cisco enable password.	“”
-d	Device password.	“”
-e	Device group description.	None
-f	Input file name for IP addresses. This specifies an ascii file that contains a list of IP addresses, one per line. No other information can be included in this file. This option can be specified more than once.	None
-g	Device group to which devices should be added. Case sensitive. The device group must already exist.	Default
-h	Input file name for device groups. This specifies an ascii file that contains a list of device group descriptions, one per line. A device group description may be included by enclosing both the device group name and the device group in double quotes. The quotes sever to delimit the two values. This option can be specified more than once.	None
-i	Device poll interval, in minutes	0
-j	SNMP version 3 privacy password	“”
-l	(Letter l) User name to use for device login	admin
-m	New device group name. Use this command when you are modifying a device group	None
-n	EPICenter server port number	8080
-o	SNMP version 3 authentication password	initialmd5
-p	EPICenter user password	“”
-r	Read community string (only needed for adding devices; not needed for deleting them).	public
-s	EPICenter server hostname or IP address	localhost
-t	SNMP version 3 authentication protocol (none, MD5, SNA)	md5
-u	EPICenter user name	None
-v	SNMP version (1, 3)	
-w	Write community string (only needed for adding devices; not needed for deleting them).	“private”
-x	Modify device setting (ssh, nussh, offline, online)	None
-y	SNMP version 3 privacy protocol (none, crc)	none
-z	Record filename (for recording)	None

Options such as the user login names and passwords and community strings, apply to all devices specified in the command. You can specify multiple devices in one command as long as they use the same options. If you have devices with different access parameters, you must add or delete them in separate commands. The exception is when removing devices or device groups, you do not need to specify community strings, so you can remove multiple devices in a single command even it their community strings are different.

Most options default to the values equivalent to those used by default on Extreme Networks devices or in the EPICenter software.

You can specify only one EPICenter server (database) in a command. If you want to add the same devices to multiple EPICenter databases, you must use a separate command for each server. The command by default adds or removes devices from the EPICenter database running on the local host at port 80.

DevCLI Examples

The following examples illustrate the usage of these commands.

- To add a device with IP address 10.205.0.99 to the EPICenter database running on server `snoopy` on port 81, with EPICenter login "master" and password "king," enter the following command:

  `devcli add -u master -p king -a 10.205.0.99 -s snoopy -n 81`

- To add two devices (10.205.0.98 and 10.205.0.99) to the EPICenter database on the local host, with read community string "read" and write community string "write," enter the following command:

  `devcli add -u admin -a 10.205.0.98 -a 10.205.0.99 -r read -w write`

- To add multiple device groups specified in the file "devGroupList.txt" to the EPICenter database, enter the following command:

  `devcli add -u admin -h devGroupList.txt`

  The file `devGroupList.txt` must be a plain ASCII text file containing one device group name and one description (if applicable) per line, such as:

  ```
  "Device Group 2"   "Marketing"
  Building B
  dg4
  ```

  If a line has multiple words delimited by white space and the words are not enclosed in double quotes, the whole line is interpreted as a device group name without a device group description. If the device group name consists of multiple words delimited by white space, and you want to specify a device group description, you must use double quotes to enclose both the device group name and the device group description.

- To modify the membership of a device group named "Engineering Device Group" to remove any existing devices from the device group and add four new devices (10.205.0.91, 10.205.0.92, 10.205.0.93, and 10.205.0.94) to the device group, enter the following command:

  `devcli mod -u admin -g "Engineering Device Group" -a 10.205.0.91 -a 10.205.0.92 -a 10.205.0.93 -a 10.205.0.94`

- To delete a set of devices specified in the file "devList.txt" with device login "admin2" and password "purple," enter the following command:

  `devcli del -u admin -f devList.txt -l admin2 -d purple`

  The file `devList.txt` must be a plain ASCII text file containing only IP addresses and only one IP address per line, such as:

  ```
  10.205.0.95
  10.205.0.96
  10.205.0.97
  ```

  If more than one IP address is specified per line, only the first IP address is used.

- To delete two device groups ("Building A" and "Building C") from the EPICenter database, enter the following command:

  `devcli del -u admin -g "Building A" -g "Building C"`

- To manually update the configurations of two devices (10.205.0.91 and 10.205.0.93), enter the command:

  devcli sync -u admin -a 10.205.0.91 -a 10.205.0.93

Inventory Export Scripts

There are three scripts you can run to export information about the devices or occupied slots known to the EPICenter inventory. The scripts let you export information on devices known to a single EPICenter installation, on slots known to a single EPICenter installation, or on devices known to multiple EPICenter servers. The information will be output in comma-separated (CSV) format suitable for importing into a spreadsheet.

- For a device report, the information reported includes the device name and type, IP address, location, serial and board numbers. If you use the Distributed server version of this report, the name of the EPICenter server that manages the device will also be included.
- For a slot report, it includes the device name and IP Address, slot number, slot name and slot type, and the serial number of the blade in the slot.

Using the Inventory Export Scripts

The three scripts are located in the EPICenter `user\scripts\bin` directory under the EPICenter install directory (by default `c:\Program Files\Extreme Networks\EPICenter 5.0` under Windows, or `/opt/extreme/epc5_0` under Solaris). You must have the `user\scripts\bin` directory as your current directory in order to run these scripts.

There are three inventory export scripts you can use:

- **`inv.bat`** <*`options`*> (Windows), or **`inv.sh`** <*`options`*> (Solaris) exports device information from the EPICenter database.

  To export device information to file `devinfo.csv` under Windows, enter the command:
  `cd “\Program Files\Extreme Networks\EPICenter 5.0\user\scripts\bin”`
  `inv.bat -o devinfo.csv`

  Under Solaris, enter the command:
  `cd /opt/extreme/epc5_0/user/scripts/bin`
  `inv.sh -o devinfo.csv`

- **`slots.bat`** <*`options`*> (Windows), or **`slots.sh`** <*`options`*> (Solaris) exports slot information from the EPICenter database.

  To run the command as user “user1,” and export slot information to file `slotinfo.csv` under Windows, enter the command:
  `cd “\Program Files\Extreme Networks\EPICenter 5.0\user\scripts\bin”`
  `slots.bat -u user1 -o slotinfo.csv`

  Under Solaris, enter the command:
  `cd /opt/extreme/epc5_0/user/scripts/bin`
  `slots.sh -u user1 -o slotinfo.csv`

- **`msinv.bat`** <*`options`*> (Windows), or **`msinv.sh`** <*`options`*> (Solaris) exports device information from the databases of multiple EPICenter servers. You must provide a list of EPICenter servers in a file.

  To export device information from the databases of EPICenter servers listed in file servers.txt (in the `scripts\config` directory) to file `alldevinfo.csv`, without prompting for a password under

Windows, enter the command:

```
cd "\Program Files\Extreme Networks\EPICenter 5.0\user\scripts\bin"
msinv.bat -d -o alldevinfo.csv -s ..\config\servers.txt
```

Under Solaris, enter the command:

```
cd /opt/extreme/epc5_0/user/scripts/bin
msinv.sh -d -o alldevinfo.csv -s ../config/servers.txt
```

The server file defaults to the file `servers.txt` in the `user\scripts\config` directory. You can edit this file to include the names or IP addresses of the servers where the EPICenter server and databases are running. You can also provide your own file. The format of the file entries are:

<servername or IP>:<port>

For example:

```
iceberg:80
10.2.3.4:81
```

Table 7 specifies the options you can use with these commands:

Table 7: Inventory script command options

Option	Value	Default
-d	None If present, the command will use the default EPICenter password ("") and will not prompt for a password.	If -p option not present, prompts for password
-n	EPICenter server port number	80
-o	Name of file to receive output. If you don't specify a path, the file will be placed in the current directory (user\scripts\bin).	output written to console (stdout)
-p	EPICenter user password	""
-u	EPICenter user name	admin
-s	For the **msinv.bat** and **msinv.sh** commands only: Name (and path) of file containing EPICenter server list	<*epc_install_dir*>\user\scripts\config\servers.txt under Windows, <*epc_install_dir*>/user/scripts/config/servrs.txt under Solaris

NOTE

The inv.bat, inv.sh, slot.bat, and slot.sh scripts retrieve information only from an EPICenter server that runs on the same machine as the scripts.

Inventory Export Examples

The following examples illustrate the usage of these commands.

- To export slot information to the file `slotinventory.csv` from the EPICenter database whose login is "admin123" and password is "sesame" under Windows, enter the following command:

  ```
  slots.bat -u admin123 -p sesame -o slotinventory.csv
  ```

  Under Solaris, enter the following command:

  ```
  slots.sh -u admin123 -p sesame -o slotinventory.csv
  ```

  This will not prompt for a password, and will output the results to the specified file.

- To export device information to the console, after prompting for a password under Windows, enter the following command:

  inv.bat

  Under Solaris, enter the following command:

  inv.sh

  This command will login with the default user name (admin), will prompt for the password, and will output the results to the console.

- To export device information to the console, using the default login and default password under Windows, enter the following command:

  inv.bat -d -o output.csv

  Under Solaris, enter the following command:

  inv.sh -d -o output.csv

  This command will login using the default user name (admin) and the default password, and will output the results to the file `output.csv` in the user\scripts\bin directory.

- To export device information from the EPICenter databases on the multiple servers under Windows, edit the `servers.txt` file in the `user\scripts\config` directory, then enter the following command:

  msinv.bat -d -o devices.csv -s serverlist2.txt

  Under Solaris, edit the `servers.txt` file in the `user/scripts/config` directory, then enter the following command:

  msinv.sh -d -o devices.csv -s serverlist2.txt

  This command logs in to each of the EPICenter servers specified in the file `serverlist2.txt`, using the default login and password, and output the device information from these servers to the file `devices.csv`. The devices.scv file is created in the user\scripts\bin directory.

The SNMPCLI Utility

The SNMPCLI utility provides three basic SNMP query capabilities, that can be used to access the values of MIB objects kept by the SNMP agents of the devices you are managing. Accessing these variable may be helpful in diagnosing problems with a device or its configuration, if its behavior as seen through the EPICenter software is not as expected.

Use of this utility assumes you are familiar with SNMP MIBs, and can determine the OID the variable you want to retrieve, as well as the meaning of the results that are returned.

NOTE

The SNMPCLI utility uses SNMP version 1.

Using the SNMPCLI Utility

The three scripts are located in the EPICenter `user\scripts\bin` directory under the EPICenter install directory (by default `\Program Files\Extreme Networks\EPICenter 5.0` under Windows, or `/opt/extreme/epc5_0` under Solaris). You must have the `user\scripts\bin` directory as your current directory in order to run these scripts.

The SNMPCLI utility supports the following three commands:

- **snmpcli snmpget** <*options*> returns the value of a specified OID.

  For example, to get the value of the object (the variable `extremePrimaryPowerOperational` in the Extreme Networks MIB) whose OID is `.1.3.6.1.4.1.1916.1.1.1.10.0` on the device at 10.205.0.99, enter the following command:
  `snmpcli snmpget -a 10.205.0.99 -o .1.3.6.1.4.1.1916.1.1.1.10.0`

- **snmpcli snmpnext** <*options*> returns the value of the next OID (subsequent to the OID you specify) in the MIB tree.

  For example, you can use this command to get the value of the object whose OID is `.1.3.6.1.4.1.1916.1.1.1.10.0` on the device at 10.205.0.99, by entering the following command:
  `snmpcli snmpnext -a 10.205.0.99 -o .1.3.6.1.4.1.1916.1.1.1.10`

- **snmpcli snmpwalk** <*options*> returns the value of the entries in a table.

  For example, to get the value of the entries in the `extremeFanStatusTable`, which is OID `.1.3.6.1.4.1.1916.1.1.1.9` on the device at 10.205.0.99, enter the following command:
  `snmpcli snmpget -a 10.205.0.99 -o .1.3.6.1.4.1.1916.1.1.1.9`

Table 8 specifies the options you can use with these commands:

Table 8: SnmpCli command options

Option	Value	Default
-a	Device IP address. This option can be specified more than once. This option is required.	None
-i	Number of indices to use when walking a MIB table (1 or 2).	1
-o	Object Identifier (OID) of the MIB object whose value you want to retrieve, or that is the starting point for the values you want. This option is required.	None
-r	Read community string	public
-t	Timeout value for SNMP request, in milliseconds.	500 ms

SNMPCLI Examples

The following examples illustrate the usage of these commands.

- To retrieve the values of the `extremePrimaryPowerOperational` and `extremeRedundantPowerStatus` variables for the Extreme Networks device with IP address 10.205.0 99, with read community string "purple" and a timeout of 1000 ms, enter the following command:

  `snmpcli snmpget -a 10.205.0.99 -r purple -t 1000 -o .1.3.6.1.4.1.1916.1.1.1.10.0 -o .1.3.6.1.4.1.1916.1.1.1.11.0`

  This returns the following:

```
IP Address: 10.205.0.99
Read community string: purple
Timeout(ms): 1000
OUTPUT:
OID: .1.3.6.1.4.1.1916.1.1.1.10.0 ;  VALUE: 1
OID: .1.3.6.1.4.1.1916.1.1.1.11.0 ;  VALUE: 1
```

- To retrieve the values from the `extremeFanStatusTable` variables for the Extreme Networks device with IP address 10.205.0.99, with the default read community string (public) and a default timeout, enter the following command:

  `snmpcli snmpwalk -a 10.205.0.99 -o .1.3.6.1.4.1.1916.1.1.1.9`

  This returns the following:

```
IP Address: 10.205.0.99
Read community string: public
Timeout(ms): 500
OUTPUT:
OID: .1.3.6.1.4.1.1916.1.1.1.9.1.1.1 ;  VALUE: 1
OID: .1.3.6.1.4.1.1916.1.1.1.9.1.1.2 ;  VALUE: 2
OID: .1.3.6.1.4.1.1916.1.1.1.9.1.1.3 ;  VALUE: 3
OID: .1.3.6.1.4.1.1916.1.1.1.9.1.2.1 ;  VALUE: 2
OID: .1.3.6.1.4.1.1916.1.1.1.9.1.2.2 ;  VALUE: 2
OID: .1.3.6.1.4.1.1916.1.1.1.9.1.2.3 ;  VALUE: 2
```

Port Configuration Utility

The Port Configuration utility is a stand-alone utility that runs on the Windows 2000, or Windows XP platform.

The EPICenter Port Configuration utility provides a way for an EPICenter administrator to change some of EPICenter's logical TCP/IP port numbers, in the event that there are conflicts between these port numbers and those used by other software products running on the same system. Because these port conflicts may prevent EPICenter from running, the port configuration capability needs to be accessible outside of EPICenter. The Port Configuration application runs on the same system as the EPICenter Database Server and Web Server.

You can run the utility from the **Programs** menu. You do not need to shut down the EPICenter services (Web Server or database) in order to change the port configurations. However, the new configurations will not take effect until you restart the affected server(s).

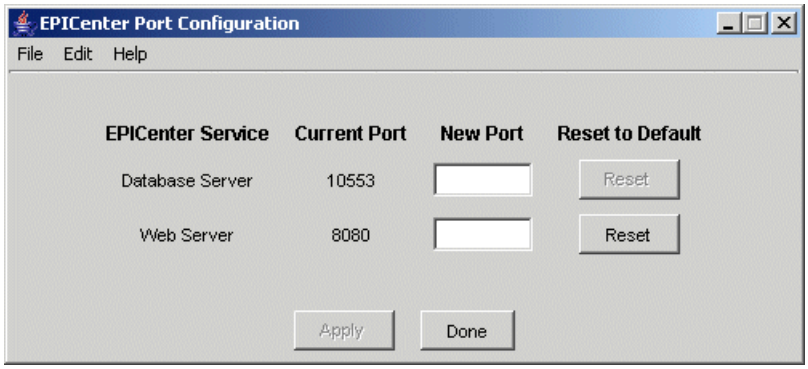
To run the Port Configuration utility, do the following:

1 Run the program from the Windows **Start** menu:

  Select **Programs**, then **Extreme Networks**, followed by **EPICenter 5.0**, then **Port Configuration**.

  The EPICenter Port Configuration window appears, as shown in Figure 72.

Figure 72: EPICenter Port Configuration Utility



2 Type in new port values for the ports you want to change.

You can use the standard Windows Cut, Copy, and Paste functions from the Edit menu, or use the keyboard shortcuts ([Ctrl]+X, [Ctrl]+C, and [Ctrl]+V) to move values among the fields.

The **Apply** button is enabled when there is text in some edit field.

3 Click **Apply** to record the settings you have entered.

Click the **Reset** button for a specific port to reset that port to its default value. The **Reset** button for a field is enabled when the corresponding values in the "Current port value" field is something other than the default.

Click **Done** when you have finished making and applying changes. Any new text in the edit fields, that has not been applied, is discarded.

The utility checks to see if it can open the requested new port number(s). If the new port number is in use, the utility reports this fact and asks if you want to keep the new value anyway.

4 To have the new port settings take effect, restart the server(s) whose ports you have changed.

Changes do not take effect until the corresponding service is stopped and restarted.

However, after applying the new values, the entries under "Current port value" are updated. This information can be misleading if you have not yet restarted the corresponding services. In particular, if you dismiss and re-run the Port Configuration utility before you restart the affected services, the "Current port value" fields will reflect the changed values which are not yet in effect.

If the servers are running as system services, you can restart your system, or stop and restart the servers using the Services utility from the Windows Control Panel.

If the EPICenter servers are not running as Windows system services, you must manually stop and restart the servers.

The AlarmMgr Utility

The Alarm Manager utility (AlarmMgr) enables you to access EPICenter alarm information and output the results to a command window or to a file. This command provides a command-line version of part of the functionality available in the EPICenter Alarm Manager applet.

Using the AlarmMgr Command

The AlarmMgr utility is located in the EPICenter `bin` directory, `<EPICenter_install_dir>/bin`. By default this is `\Program Files\Extreme Networks\EPICenter 5.0\bin` in Windows, or `/opt/extreme/epc5_0/bin` in a UNIX environment.

This command includes options for specifying EPICenter server access information and alarm filtering parameters.

The syntax of the command is as follows:

`AlarmMgr -user` *`<EPICenter username> <options>`*

The EPICenter user name is required. All other parameters are optional.

The basic command displays information about the last 300 alarms in the EPICenter database. By using filtering options, you can display information about selected alarms. You can specify a time period of interest as well as characteristics of the alarms you want to include.

You can select alarms based on criteria such as the alarm name, severity, category, source (the IP address or IP address and port that generated the alarm) and whether the alarm has been acknowledged. You can combine many of these criteria so that only alarms that meet all your criteria will be included in the results. For example, you may want to display only critical alarms from a specific device, or all alarms in a specific category that are not acknowledged.

Table 9 specifies the options you can use with this command:

Table 9: AlarmMgr command options

Option	Value		Default
-user <*username*>	EPICenter user name. This option is required.		None
-password <*password*>	EPICenter user password. If the password is blank, do not include this argument.		No password
-host <*hostname* | *IP address*>	EPICenter server hostname or IP address		localhost
-port <*port*>	EPICenter server port number		80
-h <*N*>	Display alarms that occurred within the last N hours	These options are mutually exclusive and may not be combined	Last 300 alarms
-d <*N*>	Display alarms that occurred N days ago		
-y	Display alarms that occurred yesterday		

Table 9: AlarmMgr command options (continued)

Option	Value		Default
-c <*category*>	Display alarms that occur for a specific category. Category specification is case insensitive. Must be quoted if category name includes spaces or other delimiters.	When these options are combined, an alarm must meet all criteria to be included in the results. Each of these options may be specified only once.	All categories
-s <*severity*>	Display alarms that occur for a specific severity. Severity specification is case insensitive.		All severity levels
-dip <*IP address*>	Display alarms that occur for a specific device as specified by IP address.		All devices
-p <*port*>	Display alarms that occur for a specific port on the device specified with the -dip option.		All ports
-an <*alarm name*>	Display alarms that occur for a specific alarm. Alarm name specification is case insensitive. Must be quoted if alarm name includes spaces or other delimiters.		All alarms
-a	Display all acknowledged alarms.		All alarms
-u	Display all unacknowledged alarms.		
-f <*file specification*>	Name of file to receive output. If you do not specify a path, the file is placed in the current directory. If the file already exists, it is overwritten.		Command window (stdout).
-help	Displays syntax for this command		None

- You can specify only one EPICenter server (database) in a command. If you want to display alarms from multiple EPICenter databases, you must use a separate command for each server.
- The options for specifying the relevant time period (`-h`, `-d`, and `-y`) are mutually exclusive and cannot be combined.
- You can specify filter options such as an alarm name or device (IP address) only once per command. If you want to display information for a several values of a filter option, such as several alarm names, devices, severity levels, etc., you must execute an AlarmMgr command for each value of the filter option. For example, to display alarms for two different devices, you must execute two AlarmMgr commands.
- If you specify multiple filter options, they are combined in the manner of a logical AND. This means that an alarm entry must meet all the specified criteria to be included in the command results.
- The options for specifying the relevant time period are mutually exclusive and cannot be combined.
- You should not combine the `-a` and `-u` options (for acknowledged and unacknowledged alarms). This combination indicates you want to display alarms that are both acknowledged and unacknowledged. However, there are no alarms that meet this criteria since an alarm cannot be both. To display both alarms that are acknowledged and alarms that are unacknowledged, do not specify either option.

AlarmMgr Output

The output from the AlarmMgr command is displayed as tab-delimited ascii text, one line per alarm. Each line contains the following information:

ID	Event ID of the alarm (assigned by the EPICenter server when the alarm is received)
Name	Name of the alarm
Category	Category that the alarm is classified under
Severity	Severity level of the alarm
Source	IP address of the device that generated the alarm
Time	Time the alarm occurred, reported as Greenwich Mean Time
Message	Message associated with the alarm
Acked	Whether the alarm has been acknowledged (true or false)

AlarmMgr Examples

The following examples illustrate the usage of these commands.

- To display the last 300 alarm log entries in the EPICenter database running on the local server, as user admin with the default password, enter the following command:

  ```
  AlarmMgr -user admin
  ```

- To display the last 300 alarm log entries in the EPICenter database running on server `snoopy` on port 81, with EPICenter login “master” and password “king,” enter the following command:

  ```
  AlarmMgr -host snoopy -port 81 -user master -password king
  ```

- To display all alarm log entries for the alarm named FanFailed in the local EPICenter database that occurred yesterday and are unacknowledged, enter the following command:

  ```
  AlarmMgr -user admin -y -u -an “Fan Failed”
  ```

- To find all alarm log entries that were generated from port 12 on device 10.2.3.4, and place the results in the file *device1.txt* enter the following command:

  ```
  AlarmMgr -user admin -dip 10.2.3.4 -p 12 -f device1.txt
  ```

The FindAddr Utility

Using the Find Address command (FindAddr) you can specify a Media Access Control (MAC) or Internet Protocol (IP) network address, and a set of network devices (or ports on a device) to query for those addresses. The command returns a list of the devices and ports associated with those addresses, and output the results to the command window or to a file.

This command provides a command-line version of the functionality available in the EPICenter IP/MAC Address Finder applet.

Using the FindAddr Command

The FindAddr utility is located in the EPICenter `bin` directory, `<EPICenter_install_dir>/bin`. By default this is `\Program Files\Extreme Networks\EPICenter 5.0\bin` in Windows, or `/opt/extreme/epc5_0/bin` in a UNIX environment.

This command includes options for specifying EPICenter server access information, the address to be located, and a search domain (an individual device and ports, or a device or port group).

The syntax of the command is as follows:

`FindAddr -user` *`<EPICenter username> <address options> <search domain options> <other options>`*

The EPICenter user name is required. You must also include at least one search address specification, and a search domain specification.

The FindAddr command returns a list of MAC and IP addresses and the devices and ports associated with those addresses.

Table 10 specifies the options you can use with this command:

Table 10: FindAddr command options

Option	Value		Default
-user <*username*>	EPICenter user name. This option is required.		None
-password <*password*>	EPICenter user password. If the password is blank, do not include this argument.		No password
-host <*hostname* | *IP address*>	EPICenter server hostname or IP address.		localhost
-port <*port*>	EPICenter server port number. Do not specify this after the -dip option or it will be taken as a search domain specification.		80
-f <*file specification*>	Name of file to receive output. If you do not specify a path, the file is placed in the current directory. If the file already exists, it is overwritten.		Command window (stdout)
-help	Displays syntax for this command.		None
Search address options:			
-all	Display all addresses located in the search domain.	At least one of these options is required. The -mac and -ip options may be combined.	None
-mac <*mac_address*>	Locate the specified MAC address. The address must be specified as six two-digit hexadecimal values separated by colons (xx:xx:xx:xx:xx:xx). You can specify a wildcard address by specifying asterisks instead of the last three values (for example, 21:14:18:*:*:*). This option may be repeated.		
-ip <*IP address*>	Locate the specified IP address. This option may be repeated.		

Table 10: FindAddr command options (continued)

Option	Value		Default
Search domain options:			
-dg <*device group*>	Defines the search domain to include the specified device group.	At least one of -dip, -dg, or -pg must be provided. These options may be repeated and combined.	None
-pg <*port group*>	Defines the search domain to include the specified port group.		
-dip <*IP address*>	Defines the search domain to include the device specified by the IP address.		
-port <*port*>	Defines the search domain to include one or more ports on the device specified by the -dip option. Multiple ports can be specified separated by commas. Slot and port are specified as slot:port. For example, 1:2,2:3 **Important:** If used, this option must immediately follow the -dip option to which it applies.		All ports on the device

- You can specify only one EPICenter server (database) in a command. If you want to search devices from the inventory databases of multiple EPICenter servers, you must use a separate command for each server.
- You can specify multiple IP and MAC addresses as search items by repeating the `-ip` or `-mac` options.
  - For MAC addresses, you can specify a wildcard for the last three values in the address (such as 10:11:12:*:*:*).
  - Wildcards are not supported for IP addresses. To search for multiple IP addresses, you can use the `-all` option, or include multiple `-ip` options.
  - You can specify both an IP address and a MAC address as search addresses in one command.
- You can specify each search domain option multiple times.
  - Wildcards are not supported for device IP addresses. To include multiple devices in the search domain, you can specify a device group that contains the devices, or specify multiple -dip options.
  - To restrict the search domain to one or more ports on a device, *specify the* `-port` *option immediately after the* `-dip` *option.* If you place it anywhere else in the command, it will be taken as the server port specification.
  - You can specify individual devices, device groups, and port groups in a single command.

FindAddr Output

The output from the FindAddr command is displayed as tab-delimited text, one line per address. Each line contains the following information:

- Both the MAC address and the corresponding IP address.
- The switch and port to which the address is connected.
- The user (name) currently logged in at that address, if applicable.

The output also tells you the total number of addresses found, and lists any switches in the search domain that were unreachable.

FindAddr Examples

The following examples illustrate the usage of these commands.

- To display all addresses that can be accessed through devices in the Default device group, from the local EPICenter database (with default user, password and port), enter the following command:

  FindAddr -user admin -all -dg Default

- To display all addresses that can be accessed through device 10.20.30.40, ports 5,6,7,8, in the EPICenter database running on server snoopy on port 81, with EPICenter login "master" and password "king," enter the following command:

  FindAddr -host snoopy -port 81 -user master -password king -dip 10.20.30.40 -port 5,6,7,8 -all

  Note that the second -port option immediately follows the -dip option. It must be placed in this position to specify ports as the search domain.

- To search for MAC addresses beginning with 00-01-03, and write the results to the file "info.txt," with the Default device group as the search domain, enter the following command:

  FindAddr -user admin -mac 00:01:03:*:*:* -dg Default -f info.txt

  If the file does not already exist, it will be created, by default in the EPICenter bin directory.

The TransferMgr Utility

The Transfer Manager utility (TransferMgr) allows you to upload configuration information from a device to a file, and to download configuration information and ExtremeWare software images to Extreme devices.

This command provides a command-line version of some of the functionality available in the EPICenter Configuration Manager applet.

Using the TransferMgr Command

The TransferMgr utility is located in the EPICenter bin directory, <*EPICenter_install_dir*>/bin. By default this is \Program Files\Extreme Networks\EPICenter 5.0\bin in Windows, or /opt/extreme/epc5_0/bin in a UNIX environment.

This command includes options for specifying EPICenter server access information, the transfer function to be performed (upload, download, incremental download, or ExtremeWare image download), the device on which to perform the operation on, and the file location on the server.

The syntax of the command is as follows:

TransferMgr -user <*EPICenter username*> **-upload -dip** <*device address*> <*upload location options*>

TransferMgr -user <*EPICenter username*> **-download** <*filename*>
-dip <*device address*>

TransferMgr -user <*EPICenter username*> **-incremental** <*filename*>
-dip <*device address*>

TransferMgr -user <*EPICenter username*> **-software** <*filename*>
-dip <*device address*> {primary | secondary}

The EPICenter user name, one of the four transfer options, and a device IP address are required. Other options are optional.

Table 11 specifies the options you can use with this command:

Table 11: TransferMgr command options

Option	Value	Default
-user <*username*>	EPICenter user name. This option is required.	None
-password <*password*>	EPICenter user password. If the password is blank, do not include this argument.	No password
-host <*hostname* | *IP address*>	EPICenter server hostname or IP address	localhost
-port <*port*>	EPICenter server port number	80
-help	Displays syntax for this command	None
Upload configuration:		
-upload	Upload configuration from the device specified with the -dip option.	None
-dip <*IP address*>	IP address of device from which configuration should be uploaded. This option is required, and may be repeated.	None
-ft <*string*>	Text string to be appended to device IP address to create a file name (in the format xx_xx_xx_xx.string).	<*ipaddress*>.txt (xx_xx_xx_xx.txt)
-fl <*directory*>	Directory or path below the configs directory where the upload file should be placed. <*tftp_root*> is the location of your TFTP server. By default, <*tftp_root*> is <*EPICenter_install_dir*>*user**tftp*.	<*tftp_root*>\configs
-a	Place upload file into the archive directory (<*tftp_root*>*configs*\<*year*>\<*month*>\<*day*>\<*ipaddress*>_<*time*>.txt This option may not be combined with the -fl and -ft options.	<*tftp_root*>\configs\<*ipaddress*>.txt
Download configuration:		
-download <*filename* | *path and filename*>	Download configuration from the specified file to the device specified with the -dip option. The specified file must be located in or below the <*tftp_root*>\configs directory. By default, <*tftp_root*> is <*EPICenter_install_dir*>*user**tftp*.	None
-dip <*IP address*>	IP address of device to which configuration should be downloaded. This option is required. It may *not* be repeated.	None
Download Incremental configuration:		
-incremental <*filename*>	Download an incremental configuration from the specified file to the device specified with the -dip option. The specified file must be located in the <*tftp_root*>\baselines directory. By default, <*tftp_root*> is <*EPICenter_install_dir*>*user**tftp*.	None
-dip <*IP address*>	IP address of device to which configuration should be downloaded. This option is required. It may *not* be repeated.	None

Table 11: TransferMgr command options (continued)

Option	Value	Default
Download ExtremeWare software image:		
-software <*filename* | *path and filename*>	Download a software image from the specified file to the device specified with the -dip option. The specified file must be located in the <*tftp_root*>\images directory. By default, <*tftp_root*> is <*EPICenter_install_dir*>*user**tftp*. **Important:** Make sure the software version is compatible with the switch to which you are downloading.	None
-dip <*IP address*>	IP address of device to which the image should be downloaded. This option is required. It may *not* be repeated.	None
-primary	Download to the primary image location.	Current location
-secondary	Download to the secondary image location.	

- You can specify only one EPICenter server (database) in a command. If you want to upload or download to or from devices managed by multiple EPICenter servers, you must use a separate command for each server.
- Configuration and image files are all stored in subdirectories of the EPICenter TFTP root directory, which is by default `<EPICenter_install_dir>\user\tftp`. You can change the location of the TFTP root directory by using the **Server** function of the EPICenter Configuration Manager applet.
- Standard ExtremeWare software images as shipped by Extreme Networks are provided in the directory `<EPICenter_install_dir>\user\tftp\images` directory (by default `\Program Files\Extreme Networks\EPICenter 5.0\user\tftp\images` in the Windows operating environment, or `/opt/extreme/epc5_0/user/tftp/images` on a Solaris system).

  NOTE

  Make sure the software version you download is compatible with the switch. If you download an incompatible version, the switch may not function properly.

- For uploading, you can specify multiple devices in one command. For the download options (`-download`, `-incremental`, and `-software`) you can specify only one device per command. If you want to download to multiple devices, you must execute multiple TransferMgr commands.

TransferMgr Examples

The following examples illustrate the usage of these commands.

- To upload configuration information from device 10.20.30.40, enter the following command:

  `TransferMgr -user admin -upload -dip 10.20.30.40`

  This will place the device configuration information in the file `10_20_30_40.txt` in the `configs` directory under the TFTP root directory (by default `\Program Files\Extreme Networks\EPICenter 5.0/user/tftp/configs`).

- To upload and archive configuration information from device 10.20.30.40 managed by the EPICenter server running on host `snoopy` on port 81, with EPICenter login "master" and password "king," enter the following command:

  `TransferMgr -host snoopy -port 81 -user master -password king -upload -a -dip 10.20.30.40`

Assuming the default location for the TFTP root directory, and assuming that this command was executed on July 24, 2001 at 10:02 AM, this will place the device configuration information in the file `\Program Files\Extreme Networks\EPICenter 5.0\user\tftp\configs\2001\07\24\10_20_30_40_1002.txt`.

- To download version 6.1.8 b11 of the ExtremeWare to an *i*-series device, enter the following command:

  `TransferMgr -user admin -software v618b11.xtr -dip 10.20.30.40`

The VlanMgr Utility

The VLAN Manager utility (VlanMgr) allows you to create and delete VLANs. These commands configure the VLANs on the specified switches as well as adding the VLAN information to the EPICenter database.

Using the VlanMgr Command

The VlanMgr utility is located in the EPICenter `bin` directory, *<EPICenter_install_dir>*`/bin`. By default this is `\Program Files\Extreme Networks\EPICenter 5.0\bin` in Windows, or `/opt/extreme/epc5_0/bin` in a UNIX environment.

This command includes options for specifying EPICenter server access information, the operation to be performed (create, modify or delete), the name of the VLAN, and the devices in the VLAN with their configuration options.

The syntax of the command is as follows:

`VlanMgr -user` *<EPICenter username>* **`-create`** *<VLAN name>* **`-dip`**
<IP address> *<other options>* {**`-dip`** *<IP address>* *<other options>*} ...

`VlanMgr -user` *<EPICenter username>* **`-modify`** *<VLAN name>* **`-dip`**
<IP address> *<other options>* {**`-dip`** *<IP address>* *<other options>*} ...

`VlanMgr -user` *<EPICenter username>* **`-delete`** *<VLAN name>*

The EPICenter user name and one of the main options (`-create`, `-modify`, or `-delete`) are required. The `-dip` option is required for a create or modify command. Other options are optional.

Table 12 specifies the options you can use with this command:

Table 12: VlanMgr command options

Option	Value		Default
-user <*username*>	EPICenter user name. This option is required.		None
-password <*password*>	EPICenter user password. If the password is blank, do not include this argument.		No password
-host <*hostname* | *IP address*>	EPICenter server hostname or IP address		localhost
-port <*port*>	EPICenter server port number		80
-help	Displays syntax for this command		None
Create a new VLAN:			
-create <*VLAN name*>	Create a new VLAN of the specified name.		None
-dip <*IP address*>	IP address of device to add to VLAN. This option may be repeated.		None
-port <*ports*>	Ports to be added to VLAN as untagged ports on the device specified by the preceding -dip option.	These options must immediately follow the -dip option to which they apply. Each option may be specified once per -dip option.	No untagged ports
-tagport <*ports*>	Ports to be added to the VLAN as tagged ports on the device specified by the preceding -dip option.		No tagged ports
-ipf	Enable IP forwarding for this VLAN on the specified device.		IP forwarding disabled
-ip <*IP address*>/<*subnet mask*>	Set an IP address and submask for this VLAN on the specified device. Format is xx.xx.xx.xx/nn		No ip address
-tag <*number*>	Set a tag value for the VLAN.		Untagged
-protocol <*protocol name*>	Set protocol filter.		ANY
Modify VLAN configuration:			
-modify <*VLAN name*>	Reset the configuration of the specified VLAN to the options specified in this command.		None
-dip <*IP address*>	IP address of device to be included in the VLAN. This option may be repeated.		None

Table 12: VlanMgr command options (continued)

Option	Value		Default
-port <*ports*>	Ports to be included in the VLAN as untagged ports on the device specified by the preceding -dip option. If this option is not included, any untagged ports configured on this device will be removed from the VLAN.	These options must immediately follow the -dip option to which they apply. Each option may be specified once per -dip option.	No untagged ports
-tagport <*ports*>	Ports to be included in the VLAN as tagged ports on the device specified by the preceding -dip option. If this option is not included, any tagged ports configured on this device will be removed from the VLAN.		No tagged ports
-ipf	Enable IP forwarding for this VLAN on the specified device. If this option is not included, IP forwarding will be disabled on this device.		IP forwarding disabled
-ip <*IP address*>/<*subnet mask*>	Set an IP address and submask for this VLAN on the specified device. Format is xx.xx.xx.xx/nn. If this option is not included, the VLAN will be reconfigured without a VLAN IP address.		No IP address
-tag <*number*>	Set a tag value for the VLAN. This can be a value between 2 and 4095. If this option is not included, the VLAN will be reset to an untagged VLAN.		Untagged
-protocol <*protocol name*>	Set protocol filter. If this option is not included, the protocol will be reset to ANY.		ANY
Delete VLAN:			
-delete <*VLAN name*>	Delete the specified VLAN from all switches on which it is configured.		None

- You can specify only one EPICenter server (database) in a command. If you want to create, modify or delete VLANs for devices managed by multiple EPICenter servers, you must use a separate command for each server.
- To create a VLAN on multiple switches, use multiple `-dip` options in a single command.
- The `-modify` option effectively recreates a VLAN with only the options specified in the command. Any options not specified are reset to their defaults, and only devices specified with a `-dip` option in the modify command will be included in the VLAN.

WARNING!

Only the devices that are explicitly included in a VlanMgr modify command will be included in the modified VLAN. Any devices in the original VLAN that are not specified in the modify command will be removed from the VLAN as a result of the modify command. Any options that are not explicitly specified will be reset to their defaults.

For example, suppose you have untagged VLAN *Test1* that includes ports 2, 3,and 4 on device 10.20.30.40. To add ports 1 and 2 on device 10.20.30.50 to the VLAN, you can use the `-modify` command, but the command must specify both `-dip 10.20.30.50 -port 1,2` and `-dip 10.20.30.40 -port 2,3,4`. If you do not include device 10.20.30.40 in the command, that device and its ports will be removed from the VLAN.

VlanMgr Output

The VlanMgr command displays output indicating the progress of the command as it configures the VLAN.

VlanMgr Examples

The following examples illustrate the usage of these commands.

- To create untagged VLAN test1 consisting of untagged ports 2-5, on the switch with IP address 10.20.30.01, and add it to the EPICenter database running the local server with the default administrator name and password, enter the following command:

  `VlanMgr -user admin -create test1 -dip 10.20.30.01 -port 2,3,4,5`

  This VLAN will be created with no 802.1Q tag, protocol ANY, no IP address assigned, and IP forwarding disabled.

- To create a tagged VLAN test2 with tag 53, protocol IP, on two switches with tagged ports, IP forwarding enabled, and an IP address for the VLAN on each switch, enter the following command:

  `VlanMgr -user admin -create test2 -dip 10.201.20.35 -tagport 10,11 -ipf -ip 10.201.20.100/24 -dip 10.201.20.36 -tagport 11,12,13,14,15 -ipf -ip 10.201.20.102/24 -tag 53 -protocol ip`

  This creates the VLAN on switch 10.205.0.35 with member ports 10 and 11, VLAN IP address 10.201.20.100 and VLAN mask 255.255.255.0, and on switch 10.205.0.36 with member ports 11, 12, 13, 14 and 15, VLAN IP address 10.201.20.102 and mask 255.255.255.0.

- To add port 12 on switch 10.201.20.35 to VLAN test2, leaving the configuration otherwise unchanged, enter the following command:

  `VlanMgr -user admin -modify test2 -dip 10.201.20.35 -tagport 10,11,12 -ipf -ip 10.201.20.100/24 -dip 10.201.20.36 -tagport 11,12,13,14,15 -ipf -ip 10.201.20.102/24 -tag 53 -protocol ip`

  Note that this includes all the specifications of the original create command, with the addition of port 12 to the first -tagport option. This is necessary to preserve the VLAN configuration.

  Specifying only the changes you want to make will not have the desired results. The command `VlanMgr -user admin -modify test2 -dip 10.201.20.35 -tagport 12` will result in an error because no VLAN tag is specified, and it is illegal to add a tagged port to an untagged VLAN.

  The command `VlanMgr -user admin -modify test2 -dip 10.201.20.35 -tagport 12 -tag 53` (adding just the tag specification) will successfully add port 9 to the VLAN as a tagged port, but will remove all the other ports on that switch, change the protocol to ANY, disable IP forwarding, and will remove switch 10.205.0.36 from the VLAN.

- To remove ports 14 and 15 on switch 10.201.20.36 from VLAN test2, enter the following command:

  `VlanMgr -user admin -modify test2 -dip 10.201.20.35 -tagport 10,11 -ipf -ip 10.201.20.100/24 -dip 10.201.20.36 -tagport 11,12,13 -ipf -ip 10.201.20.102/24 -tag 53 -protocol ip`

- To remove switch 10.201.20.36 from VLAN test2, enter the following command:

  `VlanMgr -user admin -modify test2 -dip 10.201.20.35 -tagport 10,11 -ipf -ip 10.201.20.100/24 -tag 53 -protocol ip`

  This command recreates the VLAN only on switch 10.201.20.35.

The ImportResources Utility

The ImportResources utility allows you to import user and host resource definitions, and groups containing those resources, from a source external to the EPICenter system. You can import from an Windows Domain server, an NIS server, or an LDAP directory. You can also import host and user resource definitions from a tab-delimited text file.

This utility performs the same function as the Import feature in the Grouping Manager. See "Importing Resources" in Chapter 8 of the *EPICenter Reference Guide* for details on this feature.

Using the ImportResources Command

The ImportResources utility is located in the EPICenter `bin` directory, `<EPICenter_install_dir>/bin`. By default this is `\Program Files\Extreme Networks\EPICenter 5.0\bin` in Windows, or `/opt/extreme/epc5_0/bin` in a UNIX environment.

This command includes options for specifying EPICenter server access information, the operation to be performed (create, modify or delete), the name of the VLAN, and the devices in the VLAN with their configuration options.

Importing from a File. To import data from a text file, you define the resources you want to import in a tab-delimited text file. See "Importing from a File" in Chapter 8 of the *EPICenter Reference Guide* for details.

Importing from an LDAP Directory. Importing from an LDAP directory uses an import specification file that defines the following:

- The information you want to extract from the directory.
- How to map that data to groups, resources, and attributes in the EPICenter Grouping module.

The specification file must be named `LDAPConfig.txt`, and must reside in the EPICenter `user/import` directory. See "Importing from an LDAP Directory" in Chapter 8 of the *EPICenter Reference Guide* for details.

Importing from an Windows Domain Controller or NIS Server. Importing from an Windows Domain Controller or NIS server is always done from the Domain Controller or NIS server that is serving the domain for the system running the EPICenter server. The type of system you are running will determine where the EPICenter server looks for the information. See "Importing from an Windows Domain Controller or NIS Server" in Chapter 8 of the *EPICenter Reference Guide* for details.

The syntax of the ImportResources command is as follows:

```
ImportResources -user <EPICenter username> -s <source name>
[-f <file name>| -ldap | -domain ]
```

The EPICenter user name and one of the import type options (`-f`, `-ldap`, or `-domain`) are required.

Table 13 specifies the options you can use with this command:

Table 13: ImportResources command options

Option	Value	Default
-user <*username*>	EPICenter user name. This option is required.	None
-password <*password*>	EPICenter user password. If the password is blank, do not include this argument.	No password
-host <*hostname* | *IP address*>	EPICenter server hostname or IP address	localhost
-port <*port*>	EPICenter server port number	80
-help	Displays syntax for this command	None
-s <*Source name*>	A name that will identify the source of the imported resources. This name is used to create a group under which all the resources imported in this operation are placed.	None
-f <*file name*>	The name of a tab-delimited text file that contains the data to be imported. See “Importing from a File” in Chapter 8 of the *EPICenter Reference Guide* for details.	None
-ldap	Specifies that the information to be imported is from an LDAP directory. Requires a specification file named LDAPConfig.txt, that resides in the EPICenter user/import directory. See “Importing from an LDAP Directory” in Chapter 8 of the *EPICenter Reference Guide* for details.	None
-domain	Specifies that the information to be imported is from an Windows Domain Controller server or a Solaris NIS server. See “Importing from an Windows Domain Controller or NIS Server” in Chapter 8 of the *EPICenter Reference Guide* for details.	None

ImportResources Examples

The following examples illustrate the usage of these commands.

- To import resources from a tab-delimited file named `importdata.txt` into a source group named *ImportedUsers* in the EPICenter database running the local server with the default administrator name and password, enter the following command:

  `ImportResources -user admin -s ImportedUsers -f importdata.txt`

- To import resources from an LDAP directory from a LDAP server into a source group named *CorpUsers* in the EPICenter database running on host `snoopy` on port 81, with EPICenter login “master” and password “king,” enter the following command:

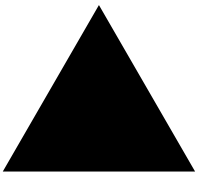
  `ImportResources -host snoopy -port 81 -user master -password king -s CorpUsers -ldap`

  This requires a configuration file named `LDAPConfig.txt` to be present in the EPICenter `user/import` directory.

- To import resources from an Windows Domain server into a source group named *NewUsers* in the EPICenter database running the local server with the default administrator name and password, enter the following command:

  `ImportResources -user admin -s NewUsers -domain`

This imports user data from the Windows Domain Controller that is serving the domain where the EPICenter server resides.



Index

Numerics

802.1Q tag 106

A

Access Domain of a policy 148
access levels. See user roles
Access List 148
access list policies 151
Access Points
  See APs
Administrator access. See user roles
alarm events
  Extreme proprietary traps 42, 120
  from EPICenter 42, 120
  SNMP traps 41, 120
Alarm Log
  Browser 42
  history 123
Alarm Log report 63
Alarm System
  description 15
  troubleshooting 173
AlarmMgr utility 19, 189
alarms
  defining 46
  definition examples 46, 50
  falling threshold for CPU utilization rules 56
  filtering the display of 43
  history 123
  predefined 41
  rising threshold for CPU utilization rules 56
  startup condition for CPU utilization 56
  startup condition for RMON alarms 54
  threshold definition 53
  tuning 120
applications as policy component 157
APs
  detecting rogue APs 112
  importing safe MAC address list 112
  performance statistics 114
architecture of EPICenter software 21
auto configuration 161
Avaya Integrated Management
  commands (table) 138
  description 133
  installation 134
  IP phones and EPICenter 139
  launching 137
  launching EPICenter 145
Avaya, discovering devices 135

B

browser-based client 166

C

Client History report 63
client Tcl API. See Tcl API
Command-line utilities 19
Config Mgmt Log report 63
configuration files
  archiving 93
  baselining 94
  detecting differences 95
Configuration Manager 16
conventions
  notice icons, About This Guide 10
  text, About This Guide 10
CPU Utilization
  alarm event generation 57
  falling threshold configuration 56
  rising threshold configuration 56
  rule definition 56
  Sample Type 56
  Startup Alarm 56
creating
  alarm definitions 46
  groups 160
Current Clients report 63

D

Debug EPICenter 64
DevCLI utility 19, 180
Device Details report 63
device groups as policy components 157
Device Inventory report 63
Device Status report 63
devices as policy components 157
devices, changing passwords 69
Disabled access. See user roles
Discovery 15
distributed server mode 20

DLCS 158
Dynamic Link Context System. See DLCS

E

EPICenter
  architecture 21
  components 20
  feature summary 13
  server components 25
EPICenter client
  description 26
  login (figure) 29
  starting in Solaris 28
  starting in Windows 27
  troubleshooting 167
EPICenter database, troubleshooting 168
EPICenter server
  performance tuning 119
  starting under Solaris 26
  starting under Windows 26
  troubleshooting 169
EPICenter Telnet. See Telnet applet
ESRP Manager
  description 18
ESRP Monitor
  troubleshooting 174
eSupport Export report 63
Event Log history 123
Event Log report 63
external access protocol 162
Extreme switch, support in EPICenter 23

F

falling threshold
  CPU utilization 56
filtering the alarm display 43
FindAddr utility 19, 191
firmware
  automated retrieval of updates 97
  detecting obsolete images 97
Firmware Manager 16

G

Grouping Manager 16, 160
groups
  as policy components 157
  creating with Grouping Manager 160
  in policy definitions 160

H

hosts as policy components 157

I

ImportResources utility 202
Interface 63
Interface report 63
inventory
  changing device information 69
  creation 65
  discovery 65
  export scripts 183
  importing devices with DevCLI 68, 69
  manually adding devices 68
  monitoring links 72
  organizing with device groups 71
  reports 74
  troubleshooting 175
  uploading to Extreme Networks TAC 75
Inventory Export script 19
Inventory Manager 15
IP address as policy components 158
IP phones
  Avaya Integrated Management 139
  display (figure) 141
  importing from Avaya Integrated Management 139
  reports 142
  syncing 141
IP Phones tab 141
IP/MAC Address Finder 16
IP-based policy 151

M

MAC polling 118
MAC spoofing 111
Macro Editor 79
Macro Player 78
Macros sub-menu 81
Manager access.See user roles
MIB poller 123
MIB Poller Summary report 64
MIB query 130
MIB Query report 64
Monitor access. See user roles

N

Navigation Toolbar 41
Network Login report 63
Network Summary Report 63
Network Summary report 63

P

policy
  definition 148
  description 148
  name 148
  precedence 161
  scope 148, 159
  traffic 153
  type 148
Policy Access Domain 159
policy components 148
  applications 157
  device groups 157
  devices 157
  groups 157
  hosts 157
  IP address 158
  policy named components 156
  policy primitive components 156
  ports 158
  QoS profiles 158
  subnets 158
  users 158
  VLANs 158
Policy Traffic 148

policy types
access-based security (QoS) 149
description 149
IP QoS (access lists) 151
Source Physical Port QoS 154
VLAN 155
Port Configuration utility 187
ports
as policy components 158
changing configuration 187
correcting conflicts 187
Power over Ethernet report 63
predefined alarms 41

Q

QoS profile as policy components 158

R

RADIUS 19
Real-Time Statistics 17
related publications, About This Guide 11
Release Notes 9
Remote Authentication Dial In User Service. See RADIUS
Reports
Network Summary Report 63
reports 18, 63
Alarm Log 63
Client History 63
Config Mgmt Log 63
Current Clients 63
Debug EPICenter 64
Device Details 63
Device Inventory report 63
Device Status report 63
eSupport Export 63
Event Log 63
MIB Poller Summary 64
MIB Query 64
Network Login 63
Network Summary report 63
Power over Ethernet 63
Resource to Attribute 64
Rogue AP Alarms 63
Rogue AP Detail report 63
Rogue APs 63
Safe AP MAC List 63
Server State Summary 64
Slot Inventory report 63
Spoofed Clients 63
Syslog 63
Unconnected Clients 63
Unused Port 63
User to Host 64
VLAN Summary 63
Voice VLAN Summary 63
Wireless AP 63
Wireless Interface report 63
Wireless Port Detail 63
Wireless Summary 63
Resource to Attribute report 64
rising threshold
CPU utilization 56
RMON
alarm event generation 55, 57
alarm examples 50
event generation (figure) 55
predefined alarms 41
Startup Alarm 54
threshold definition 53
traps 22, 41, 42
Rogue AP Alarms report 63
Rogue AP Detail report 63
Rogue APs report 63
Role-based macros 81
rule
CPU utilization threshold configuration 56
runclient command in Solaris 28
runserv command in Solaris 26

S

Safe AP MAC List report 63
safe MAC address list 112
Sample Type
Absolute (for CPU Utilization 56
Delta (for CPU Utilization) 56
security
denying TCP SYN packets 108
relevant syslog messages (table) 105
SNMPv3 100
using IP access lists 107
using VLANs 105
Server Hostname field 29
server properties
Avaya Integration 144
Server State Summary report 64
Slot Inventory report 63
SmartTraps 21, 22
SNMP
MIB query 130
polling 118
SNMPv3 for security 100
traps 21, 22, 41, 42
SNMPCLI utility 19, 185
software
architecture 21
components 20
Solaris, starting the server 26
source port policy 154
Spoofed Clients report 63
Spoofing Wireless Client Report 111
SSH 102
stand-alone client application 165
Stand-alone Utilities 19
starting the client
under Windows 27
starting the server
under Solaris 26
under Windows 26
Startup Alarm
for CPU Utilization 56
RMON 54
status poll 21
STP Monitor 18
subnets as policy components 158
Syslog report 63

T

Tcl API 162
TCP SYN packets, blocking with IP policies 108
Telnet applet 16
  example macros 79
  execution context 80
  execution role 80
terminology, About This Guide 9
third-party device support 23
Topology views 17
TransferMgr utility 19, 194
traps
  Extreme proprietary 42, 120
  RMON 22, 41, 42
  SNMP 21, 22, 41, 42
troubleshooting
  Alarm System 173
  EPICenter client 167
  EPICenter database 168
  EPICenter server 169
  ESRP Monitor 174
  Grouping Manager 176
  Inventory Manager 175
  Printing 176
  Reports 177
  STP Monitor 177
  VLAN Manager 172

U

Unconnected Clients report 63
Unused Port report 63
user roles
  administrator 19
  disabled 19
  manager access 19
  monitor access 19
  using RADIUS 100
User to Host report 64
user-defined macro variables 80
User-Defined Telnet Macros 78
users as policy components 158

V

VLAN Manager
  description 18
  troubleshooting 172
VLAN policy 155
VLAN Summary report 63
VlanMgr utility 19, 198
VLANs
  802.1Q tag 106
  as policy components 158
  creating (figure) 88
  definition of 106
  for security 105
  modifying from topology map 89
  protocol filters 106
  topology (figure) 87
  viewing misconfigurations 90
Voice VLAN Summary report 63

W

Windows
  starting the client 27
  starting the server 26
wireless
  client MAC spoofing 111
  clients with no encryption 113
  interface report 110
  monitoring unauthenticated clients 111
  Spoofing Wireless Client Report 111
  syslog reports 115
Wireless AP report 63
Wireless Interface report 63
Wireless Port Detail report 63
Wireless Summary report 63